NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

MONITORING INFORMATION SYSTEMS TO ENFORCE COMPUTER SECURITY POLICIES

by
Scott W. Graham
Stephen E. Mills

September 1999

Thesis Advisor:	Vicente Garcia
Second Reader:	James Bret Michael

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 1999	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE MONITORING INFORMATION SYSTEMS TO ENFORCE COMPUTER SECURITY POLICIES	**5. FUNDING NUMBERS**
6. AUTHOR(S) Graham, Scott W. and Mills, Stephen E.	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution unlimited.	**12b. DISTRIBUTION CODE**

13. ABSTRACT ***(maximum 200 words)***

Many computer security policies are written relatively vaguely. In many ways this is intentional to allow for easier access to all the functionality of the computer network. However, too much leeway allows users, without a need to access many of the network functions, the ability to execute functions that might cause harm to the system or provide access to information they have no need to see. With this in mind, this paper takes a look at computer security. We start with a brief history of computer security and continue with a look at internal security. Since our focus is on computer misuse and detection, a look at internal security provides a look at the reasons why we should attempt to monitor the activities of users. Misuse detection requires at least two features. These are audit reduction and profiling ability. When audit features are enabled in the operating system, massive files can build up. By establishing profiles of personnel usage, the automated audit features can quickly scan audit files, look for usage that falls outside what is determined to be normal, notify administrators, and delete old audit data. A misuse detection system, such as the Computer Misuse Detection System marketed by ODS Networks, may be implemented and incorporated into a comprehensive security policy.

14. SUBJECT TERMS Computer Security, Profiling, Computer Security Policy	**15. NUMBER OF PAGES** 138
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFI- CATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

THIS PAGE INTENTIONALLY LEFT BLANK

MONITORING INFORMATION SYSTEMS TO ENFORCE COMPUTER SECURITY POLICIES

Scott W. Graham
Lieutenant, United States Navy
B.G.S., Roosevelt University, 1989

Stephen E. Mills
Lieutenant, United States Navy
B.S., Old Dominion University, 1992

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
September 1999

Authors: Scott W Graham
Scott W. Graham

Stephen E. Mills

Approved by: Vicente Garcia
Vicente Garcia, Thesis Advisor

James Bret Michael
James Bret Michael, Second Reader

Dan C Boger
Dan Boger, Chairman
Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Many computer security policies are written relatively vaguely. In many ways this is intentional to allow for easier access to all the functionality of the computer network. However, too much leeway allows users, without a need to access many of the network functions, the ability to execute functions that might cause harm to the system or provide access to information they have no need to see. With this in mind, this paper takes a look at computer security. We start with a brief history of computer security and continue with a look at internal security. Since our focus is on computer misuse and detection, a look at internal security provides a look at the reasons why we should attempt to monitor the activities of users. Misuse detection requires at least two features. These are audit reduction and profiling ability. When audit features are enabled in the operating system, massive files can build up. By establishing profiles of personnel usage, the automated audit features can quickly scan audit files, look for usage that falls outside what is determined to be normal, notify administrators, and delete old audit data. A misuse detection system, such as the Computer Misuse Detection System marketed by ODS Networks, may be implemented and incorporated into a comprehensive security policy.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION

A. BACKGROUND

As the end of the twentieth century approaches, the world finds itself in the middle of a technological revolution with ever increasing dependence on computers and computer systems. With this increasing dependence, the need to protect these systems and the data contained within their databases has become a major priority for governments and private industry. Recognizing the need to develop infrastructure protection, the President of the United States signed Executive Order 13010 on July 15, 1996 outlining a plan for dealing with critical infrastructure protection. It states that "Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."

The Presidential Decision Directive 63 (PPD 63), Protecting America's Critical Infrastructures, builds on the recommendations of Executive Order 13010. Signed in October of 1997, this report calls for a national effort to assure the security of the United States increasingly vulnerable and interconnected infrastructures. PPD 63 is a culmination of an intense, interagency effort to evaluate and act on the recommendations of Executive Order 13010 and produce a workable and innovative framework for critical infrastructure protection.

One aspect of this infrastructure protection is a need to correctly identify personnel who have access to sensitive information and prevent the ones that do not have access to this information. With the ever-increasing connectivity among networks internal to an enterprise and between enterprises, the concept of user profiling has continued to evolve. Profiling is not new, and has been used in many fields other than information systems management. Federal Government agencies have become extremely interested in developing user level computer profiling for their ever-increasing databases of groups, subgroups, and individual users.

A well-defined computer security policy is the foundation of a successful security program. Therefore, in order to take advantage of the potential power of having access to user profiles, it is of paramount importance that profiling be incorporated into an organization's computer security policy. The incorporation of monitoring users along with periodic training will greatly enhance a systems security program.

B. OBJECTIVES

The objective of this thesis is two-fold. First, the evaluation and testing of a commercially available computer profiling software was performed to determine if the product can perform as advertised on Department of Defense type computer systems. After reviewing several software packages, we selected an exemplary application package that provided the necessary tools needed to perform user profiling. The Computer Misuse Detection System (CMDS), developed by ODS Networks Inc., provides intrusion detection, data forensics, audit management, and a comprehensive user profiling system. Our second objective was to incorporate a monitoring program into an organization’s computer security policy.

C. ORGANIZATION OF THESIS

This thesis is divided into seven chapters. Chapter II provides a detailed look at the evolution of computer history and the importance of computer security. Chapter III is a comprehensive explanation on how computer systems are penetrated from internal sources. Chapter IV takes a look at a relatively new aspect of computer security - profiling; it covers the origins of profiling and reviews many of the current applications that use profiling. A detailed overview of the Computer Misuse and Detection System (CMDS) program is provided in Chapter V. The importance of a well-defined computer security policy is explained in Chapter VI, followed by a discussion of the integration of a system monitoring program into a current computer security policy, is discussed. The conclusion and recommendations are presented in Chapter VII.

THIS PAGE INTENTIONALLY LEFT BLANK

II. HISTORY OF COMPUTER SECURITY

A. OVERVIEW

Computers are used today more than ever before to conduct business transactions, store sensitive data, and perform personal work at home. The ability to share information has greatly increased as computers become connected to networks, creating computer systems. The information contained within these computer systems is the major focus of today's computer security policies. What is this information? It is information pertaining to every detail of our lives - medical files, criminal investigation data, banking transactions, and personnel files. It is information that we desire to keep private. Every organization will have a unique computer security policy tailored to the organization's specific needs. In order to fully understand the current direction computer security is heading, with respect to profiling technology it is important to look at its modest beginnings. This chapter briefly recounts the evaluation in computing environments and the computer security that inevitably followed.

B. COMPUTER SECURITY FOUNDATIONS

The first step in developing any policy is to define the objective, in our case computer security policy. What is computer security? In simple terms - it is the protection of the computer system and all associated equipment. This includes both physical and logical stores of data.

There are three fundamental cornerstones of computer security - confidentiality, integrity, and availability. Confidentiality ensures that the data stored on a computer system is protected and released only to authorized users. It include s items such as payroll information, official email, or personnel data on employees. It has significant meaning in a military environment. For example, message traffic that is centrally stored and can be accessed by command personnel at various classification levels ranging from unclassified to top secret. It is extremely important that only personnel with the proper security clearance be able to read messages, at or below their security level.

Integrity focuses on preventing unauthorized modification of data. For example, integrity is extremely important to banking institutions, whose customers demand accuracy in the computation and storage of very financial transaction. Within the military, it is of the utmost importance to ensure that message traffic received is accurate and has not been modified by hackers. Operational commanders need to know that messages providing coordinates for missile strikes have not been modified by an unauthorized party. An inaccurate message could result in a failed mission, civilian casualties, or have significant political ramifications. Additionally, enemy hackers could intercept and falsify information such as troop numbers, location or potential attack plans.

Availability is having data and other computing resources readily accessible on demand. An Internet company would be quickly out of business if customers were unable to access data on the company's web site. Computers are the cornerstone of most military weapons systems. These systems need to have a high rate of availability in order to conduct military operations at a moment's notice.

In addition to these fundamental properties, there are many secondary concerns that must also be considered when developing a security policy, such as consistency, control, and audits. Consistency involves making sure the system behaves as expected. Control is regulating access to your system. Audits are performed to monitor the use of the system by employees as well as access by outside interests.

C. THREATS AND VULNERABILITIES

All computer systems are susceptible to certain threats and are vulnerable to some extent of attacks. Computer security is concerned with the protection of systems from various threats and identification of vulnerabilities of the system. Anything that can cause damage to a system is considered a threat. Threats fall into three distinct categories: natural, unintentional, and intentional. [Ref. 1] Natural threats are unplanned events such as fires, floods, or unexpected power surges. Unintentional threats primarily can arise due to poor security training. For example, significant threats to computer systems can come from a careless user that gives out his or her password to a friend, or a system administrator that does not fully understand the security policy or how to maintain security mechanisms (e.g., firewalls). However, there are many intentional threats out there that can cause catastrophic damage to organizations. Intentional threats can be either external or internal and come from a wide variety of sources. External threats are the ones most people are familiar with, and consist of crackers, hackers, terrorist, corporate raiders, or foreign intelligence agents. They penetrate systems using a variety of methods ranging from remote electronic break-ins to bribing employees for information. Internal threats come from personnel who have access to the system and for some reason, possibly out of malice, decide to disrupt or steal information. These threats can come from corporate spies being paid to acquire corporate secrets or simply a disgruntled employee. It has been estimated that as many as 80 percent of system penetrations come from personnel that had full access to the system performing unauthorized functions. [Ref. 1]

There is no such thing as a completely secure computer systems: every computer system has an Achilles heel. It is important to understand the vulnerabilities of a system when developing a security policy. System vulnerabilities can be divided into the following categories: [Ref. 1]

- Physical Vulnerabilities - Office building and computer rooms should be secured to prevent break-ins from intruders. Many devices are available to prevent intruders from gaining access; cipher locks, retina scans, voiceprint, fingerprint and security alarms all provide an effective deterrent.
- Natural Vulnerabilities - Natural disasters such as floods, fires or power surges that can cause loss of data.
- Software Vulnerabilities - Software failures can cause your computer system to crash. They might also contain "holes" and/or "trap doors" that can allow a hacker access to your system and information.
- Emanation Vulnerabilities - The sensitive electronic equipment that makes up a computer system is extremely vulnerable to electromagnetic attack. Additionally, all computers emit electromagnetic radiation that contains information. This information, with the proper equipment, can be collected and recorded.

- Communication Vulnerabilities - Any computer connected to a network runs the risk of being penetrated from a remote location.
- Human Vulnerabilities - Employees are the leading cause of many security problems and this makes them one of the greatest vulnerabilities to a computer system. [Ref. 1]

D. EVOLUTION OF MODERN COMPUTING ENVIRONMENTS

In the early days of computing, computer systems were large and extremely expensive. Many times entire systems were dedicated to single users or at most a select few, who simply had to clear the computer's memory, pick up their computer tapes, punch cards, and lock up the office at the end of the workday to protect both their systems and information from intruders. [Ref. 2] The user had complete control of the operating environment. Computer security was simply part of the organization's physical security plan. The organization's primary security concerns centered on physical break-ins, theft of the actual computer equipment, and theft of computer disks, tape reels, or punch cards.

Prior to the 1980's, the fear of an insider threat was of little concern to most organizations. Very few people were knowledgeable computer users and the select few that actually worked on the computers did so in secured locations. Most users never saw the computer systems that performed their everyday tasks. Users submitted screened batch processing jobs and retrieved the results.

As times changed, computer technology also evolved. During the late 1960's, users began to interact with computers more frequently and started to demand better utilization of computing resources. The computing environment began to shift from central control to decentralized computing. This change in computing paradigms provided users with more control over their computing resources, while opening the door for new possibilities for computer misuse.

The ability to access computers from remote locations revolutionized the computer age. With the increase in telecommunications, computer "networks" grew in size and complexity. Many large businesses began to automate and store information about their customers, vendors, and commercial transactions.

Network-based computer access had a dramatic impact on education. Colleges and universities throughout the country now found it possible to link themselves into large computer networks and centralized computer databases. The first major network for education and government use was the Arpanet, which later evolved into the Internet. This explosion in computer availability provided students the opportunity to experiment and work with computers for the first time. This created a "snowball" effect leading to a tremendous increase in the total number of people using computers. The mystique of an open computing environment began to slowly fade, as threats and attacks became commonplace.

The introduction of the personal computer during the 1980's provided access to an even greater number of people. The personal computer began to appear on desks in both the workplace and at home. As the price of computers began to steadily drop, many small businesses saw this as an opportunity to automate their operations to stay competitive with larger companies. The advent and availability of the personal computer presented another challenge to computer security. People could now create programs at home to steal information or disrupt operations. Moreover, data that needed to be transferred between systems was stored on diskettes and could now be easily downloaded and stolen.

During the late 1980's and early 1990's, the use of the personal computer increased at an exponential rate. As this use increased, so did the use of networks, electronic mail, and bulletin boards. These new developments in computing increased the ability of users to communicate with each other and other computer systems. This new freedom in computing opens a whole new playground for hackers. Before the wide spread use of networks, a hacker might be able to penetrate a single system at a time via a modem. Now a would-be hacker has the potential to access many systems with a single break-in and has the ability to disrupt computer systems throughout the world.

The 1990's saw the emergence of open systems as well as an increasing dependence on networks and the need to share data, applications, and hardware resources. In the past, security was not considered a major concern, but with the advent of the INTERNET, the ability to "reach out and touch" a network has gone global.

E. SECURITY EFFORTS

The earliest computer-related security activities began in the 1950's. The United States government, understanding the potential security risks related to computers, took some initial steps to protect government computing resources. The first TEMPEST (Transient Electromagnetic Pulse Emanation Standard) security standard was designed to take advantage of the fact that all electronic equipment emits signals that can be received outside the system. Additionally, the first government security organization, the United

States Communications Security (COMSEC) Board, was established to oversee the protection of classified information and consisted of representatives from many different branches of the government.

This modest attempt at providing for computer security provided the foundation upon which advances were made in computer security. The Department of Defense, National Security Agency, and the National Bureau of Standards all started security initiatives. These initiatives combined with the first public awareness of security emerged toward the late 1960's.

1. Public Awareness

The first major public awareness of computer security came from the Spring Joint Computer Conference of 1967. This conference is generally recognized as the first comprehensive computer security presentation to a technical audience. The presentation was chaired by Willis H. Ware of the RAND Corporation and addressed the complicated issues surrounding the vulnerabilities of resource sharing and remote access computer systems. Topics included electromagnetic radiation, wiretaps on communications lines, unauthorized programmers, and user access to systems and data.

2. Department of Defense Initiatives

The Department of Defense was one of the first organizations to use computer systems and had a strong interest in protecting classified information stored on these systems. In October of 1967, the Department of Defense established a task force within the Advanced Research Projects Agency (ARPA). The goal of the task force was to study various computer systems and networks, identify vulnerabilities and threats, and make recommendations for safeguarding and controlling access to Department of

Defense computers, systems, networks, and information. After over two years of examining the problem, the task force published the classified document called *Security Controls for Computer Systems* in 1970. This document was the first of it kind and was the foundation for many security programs that followed, dedicated to the protection of classified information.

The Department of Defense began to develop regulations for enforcing the security of the computer systems, networks and classified data used by the Department of Defense and government contractors, and in 1972 issued DoD directive 5200.28, *Security Requirements for Automated Data Processing (ADP) Systems*. This directive established a consistent DoD policy for computer system control and stated the following as its overall policy:

> Classified material contained in an ADP system shall be safeguarded by the continuous employment of protective features in the system's hardware and software design and configuration. [Ref. 1]

This directive was the first formal document establishing a computer security policy for an organization. It was unique in the fact it stipulated that systems specifically protect, not only the computer equipment, but also the data contained within the systems from deliberated and inadvertent access to classified material by unauthorized persons.

Throughout the 1970's many computer security initiatives were developed to better understand computer systems vulnerabilities and to find a way to combat threats. The initiatives fell into three general categories: tiger teams, security research studies, and the development of the first secure operating system.

a. Tiger Teams

The 1970's saw the emergence of government- and industry-sponsored tiger teams. The tiger teams consisted of a group of hackers who attempted to break into computer systems to identify weaknesses in security mechanisms. Once weaknesses were found, the team would develop "patches" to secure the holes. While tiger teams provide an effective way of locating vulnerabilities, the teams' efforts were often uncoordinated and could not necessarily find all the security problems that existed within any one system. Often tiger teams found security flaws that were missed by previous tiger teams. Therefore, one could not be guaranteed a secure system just because one tiger team could not penetrate the system. The tiger team concept was the first organized attempt at providing a solution to the ever-increasing problem of computer attacks. Even though tiger teams have not always been effective, they have shown how easily security flaws in systems can be exploited. They have also pressed the need for a more efficient and standardized method of testing and evaluating both security policy and its implementation.

b. Modeling

While tiger teams were busy identifying security flaws, various government agencies began sponsoring groundbreaking research projects. These projects were designed to analyze security requirements, construct security policy models, and provide recommendations to government officials. Several significant views on computer security emerged from these research projects. The first of which was the concept of a reference monitor. James P. Anderson first reported the reference monitor in the Computer Security Technology Planning Study written in 1972.

> The reference monitor enforces security by forcing all subjects who wish to access an object to do so only through the monitor itself. [Ref. 3]

The concept of a reference monitor becomes extremely important in the development of standards and technologies for a secure system. The reference monitor makes access control decisions based on a set of rules, that describes which subjects can access which objects. The rules can specify certain files or objects and will represent a synopsis of the access control policy and model chosen for the system.

Additionally, the first organized effort to establish a security policy model was by the Department of Defense, who sponsored many projects in the late 1970's focusing on the development of mathematical models of security. The two most significant of the models are known as the Bell-LaPadula model and the Clark-Wilson model.

The Bell and LaPadula model was of great interest to the Department of Defense because it enforced the military's goal to eliminate unauthorized disclosure and provide for the declassification of sensitive information. While this model was extremely useful for military computer systems, it posed many challenges for commercial organizations whose processing of sensitive information differed substantially from that of the military and intelligence communities.

To address the needs of the commercial industry, David Clark and David Wilson developed a security model that focused on the integrity of the information rather than its actual disclosure. As more businesses started to rely on commercial data processing to keep track of their financial records, it became necessary to prevent unauthorized modification of that data. It uses two types of mechanisms to accomplish this goal: well-formed transactions and separation of duties.

The well-formed transaction is an electronic audit log that ensures users cannot randomly change data. This gives the system administrator the ability to recreate the actions of a user in the event of a computer security breach and restore the original data if needed. Audit logs do not physically stop a would-be intruder from accessing and changing data, but the knowledge a system exists can be a deterrent.

The second mechanism used in the Clark-Wilson model is separation of duty. The goal of separation of duty is to maintain the integrity of data by separating the operations required to modify the data into several parts and requiring that different users perform each part. By increasing the number of employees required to complete task, it increases the difficulty of committing fraud without being caught.

The purpose of this model is not only to stop unauthorized users from modifying sensitive accounting and financial data, it also addresses issues related to authorized users that have access to sensitive information. While computer security, up to this point in history, was focused on denying access from outside threats, this was the first significant attempt in combating the insider threat.

As time went on, other models were developed to address more specific security concerns. For example, the Goguen-Meseguer model addressed the issue of noninterference between subjects. It is designed to prevent users from interfering with one another.

c. *The Development of Trusted Computer Systems*

While many government-sponsored projects focused on the development of security models in the early 1970's, others began to develop the first trusted systems. The key to developing a trusted system is the security kernel. The security kernel is the part of the operating system that controls access to all of the computer resources and is the bottom layer in a multi-layer system design. The formal definition of the security kernel as defined in the "Orange Book" is:

> The hardware, firmware, and software elements of a Trusted Computing Base that implement the reference monitor concept. It must mediate all access, be protected from modification, and be verifiable as correct. [Ref. 1]

The most significant development of the security kernel came from an Air Force sponsored project for the Multics (Multiplexed Information and Computing System) System. The Multics System is significant in the fact that it allows users with different security clearances to simultaneously access information that has been classified at different levels and was extremely important in the development of future trusted systems. It features a large-scale highly interactive computer system that provides extensive password and login controls. Additional features include the following: data security through access control lists (ACLs), an access isolation mechanism (AIM), auditing of all system access operations, decentralized system administration, segmented virtual memory, and a stacked-controlled process architecture.

F. STANDARDIZATION

Toward the end of the 1970's, the need for standards was recognized as being of paramount importance. As a result, two significant government initiatives were started to conduct research in the area of computer security standards. The first initiative was started in 1977 and was simply titled the DoD Computer Security Initiative. The primary goal of this initiative was to bring computer security into the national spotlight. A series of seminars conducted in 1978 set out to answer questions relating to computer security.

As a result of this initiative, the National Security Agency (NSA) was given the additional responsibility of information security. The Computer Security Center (CSC) was created within NSA to expand on the Computer Security Initiative. The CSC became known as the National Computer Security Center (NCSC) in 1985 and its role was expanded to include all federal agencies having the following goals: [Ref. 4]

- Encourage the widespread availability of trusted computer systems.
- Evaluate the technical protection capabilities of industry and government developed systems.
- Provide technical support of government and industry groups engaged in computer security research and development.
- Develop technical criteria for the evaluation of computer systems.
- Evaluate commercial systems.
- Conduct and sponsor research in computer and network security technology.
- Develop and provide access to verification and analysis tools used to develop and test secure computer systems.

- Conduct training in areas of computer security.
- Disseminate computer security information to other branches of the federal government and to industry.

One of the most important publications by the NCSC was the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), commonly known as the "Orange Book." The Orange Book has been widely considered the bible of secure system development. [Ref. 1] It was the first publication to address the evaluation criteria used to access the level of trust that can be placed in a computer system. It effectively makes security a measurable commodity by determining the exact level of security a system needs. The Orange Book defines specific levels of security protection, D, C, B, and A, in order of increasing security. These levels are further divided into one or more classes, with each class having a specific set of criteria that the system must meet in order to obtain the rating for that class.

The second initiative came from the National Bureau of Standards (NBS). In 1977 the NBS started a series of Invitational Workshops dedicated to the Audit and Evaluation of Computer Systems. The goal of the first workshop was to determine:

> What authoritative ways exists, or should exist, to decide whether a particular computer system is "secure enough" for a particular intended environment or operation, and if a given system is not "secure enough," what measures could or should be taken to do so. [Ref. 1]

The members of the workshop considered many aspects of computer security before making their recommendation. The final conclusion of the workshop stated:

> By any reasonable definition of "secure" no current operating system today can be considered "secure"...We hope the reader does not interpret this to mean that highly sensitive information cannot be dealt with

> securely in a computer, for of course that is done all the time. The point is that the internal control mechanisms of current operating systems have too low integrity for them to...effectively isolate a user on the system from data that is at a "higher" security than he is trusted...to deal with. [Ref. 1]

Many significant recommendations came from the NBS workshops. They determined that sensitive government information not covered by national security guidelines required a detailed computer security policy. Additionally, the workshop attendees identified the need for formal evaluation and accreditation process for information systems that manage sensitive information. The most significant recommendation was to establish a standard method of measuring the overall security of a computer system.

While the NCSC and NBS were pioneers in the development of computer security standards, many other standards were authored and had a significant impact on the realization of trusted computing. Major advances in cryptography, electromagnetic radiation, biometrics and other enabling technologies have all helped to reduce the susceptibility of information systems to threats and vulnerabilities.

G. LEGISLATION ADDRESSING COMPUTER SECURITY

Legislation has been passed over the years dealing with both computer crime and the protection of classified and sensitive information. The legislation has influenced the way computer security is addressed both in the public and private sectors. Computer crime legislation began during the infant stage of computer development and continues today.

In addition to the numerous U.S. Codes dealing with computer crime, many laws have been enacted that specifically deal with the protection of classified and sensitive information. These laws were a direct result of the ever-increasing national awareness of the importance of computer security.

The National Security Decision Directive 145 (NSDD 145) of 1984 had a tremendous effect on the world of computer security. Not only did it mandated protection of both classified and sensitive information, it also empowered the NSA to "encourage, advise and if appropriate assist" the private sector. Specifically, it requires all computer systems that handle classified or sensitive information be protected against unauthorized access. While classified information is pretty well defined, sensitive information would include such things as productivity statistics, information that could disrupt public services, and all information collected from the Social Security Administration, Federal Bureau of Investigation, Internal Revenue Service, and the Census Bureau. In addition to protecting classified information, NSDD 145 created a System Security Steering Group that consists of members from the DoD, Attorney General's Office, State Department, Treasury Department, Office of Management and Budget, Federal Bureau of Investigation as well as many others. This interagency group manages computer security within the government and provides policy and guidance to all government agencies.

The National Telecommunications and Information System Security Publication 2 (NTISSP 2) was developed to better define "sensitive but unclassified" information. It basically states that "sensitive but unclassified" information is information that could adversely affect national security. The NTISSP 2 applies to all government agencies and contractors and allows the agency itself to determine what information is "sensitive but unclassified" and to provide adequate protection of this information.

In an effort to further protect sensitive government information, the Computer Security Act of 1988 went into effect. It requires that a customized security plan be developed for all U.S. government computer systems that contain sensitive information. Additionally, it requires that all government employees that have access to computer systems that contain sensitive information receive formal training in the field of computer security.

H. SUMMARY

The modern computing environment shows little resemblance to its predecessor of the 1950's. Today's computing relies on huge computer networks that transfer large quantities of information between systems. The speed in which information can be processed and transferred is always increasing and a need to protect this sensitive information is a major concern among government agencies and private organizations. Computer systems are vulnerable to various threats including; physical threats, natural threats, software-related attacks, and electronic attacks. To combat these costly attacks, many computer security initiatives were developed. The earliest computer-related security activity began in the 1950's with the TEMPEST standard. The United States government founded its first security organization, the COMSEC board, to oversee the protection of classified information. During the late 1970's, the need for standards was determined to be of the utmost importance. Throughout the 1980's and 1990's many computer related standards were developed and numerous legislation was passed to help ensure the protection of sensitive information. Recently, two significant pieces of legislation were enacted to develop infrastructure protection within the United States. Executive Order 13010 outlines a plan to deal with infrastructure protection and PPD 63 calls for an interagency effort to evaluate past recommendations and create a framework for critical infrastructure protection.

THIS PAGE INTENTIONALLY LEFT BLANK

III. INTERNAL THREAT

A. INTRODUCTION

Bruce Schneier, author of the book *E-mail Security* and President of Counterpane Systems said:

> The only secure computer is one that is turned off, locked in a safe, buried 20 feet down in a secret location - and I'm not completely confident of that one either.

However, if we were to lock our computers away, no work would be accomplished by utilizing them. As an advanced society we have become increasingly dependent on information systems. We must find a way to keep them safe and secure—not only from outsiders, but insiders as well.

Insiders are legitimate users of a computer. They use their knowledge to circumvent computer security protection and are likely to have specific goals and objectives as well as the ability to determine the best method to attain their objective based on their knowledge of the system. In a recent survey of security managers, more than 24 percent of those asked stated that the primary threat affecting their systems was insiders. [Ref. 5]

According to a 1998 survey by the Computer Security Institute, approximately 70 percent of organizations polled reported that their networks had been penetrated. About 67 percent of these attacks were from inside the network. So it appears that a network would have a 33 per cent chance of penetration from outside the network, and a 67 per cent chance of penetration, or abuse, from inside the network. Yet most of the research into protecting information from harm has been placed on protection from "outsiders". [Ref. 5]

The February 28, 1994 Joint Security Commission report to the Secretary of Defense and the Director of Central Intelligence found that: "The great majority of past compromises have involved insiders, cleared persons with authorized access who could circumvent physical security barriers, not outsiders breaking into secure areas."

The commission highlighted two areas that they felt required particular attention: Personnel security and the trustworthiness of those who deal with sensitive information and Information Systems security requires increased attention. [Ref. 6]

B. WHO REPRESENTS THE INSIDER THREAT?

1. The Espionage Threat

Spies are generally paid informants that infiltrate computer systems from the inside for the purpose of selling the information to competitors, or foreign governments, for profit. Information brokers have paid employees with access to provide data on unpublished telephone numbers, toll records, credit reports, and other personal information. [Ref. 5] In the case of government information, the information is passed to foreign governments. Weather it is industrial, technical, or military information, these activities are illegal.

2. Disgruntled Employees

Disgruntled employees can be extremely damaging to a network. Of particular danger is when someone with excessive knowledge of your system, such as a system administrator, decides to cause harm. A computer systems administrator for a large defense contractor in California planted a logic bomb in one of the computer systems used by the corporation in the development of advanced weapons systems. The employee was due to be terminated and had set up the malicious code to activate after his departure. He hoped that the company would hire him back to reconstruct databases after the logic bomb functioned. His attempt was discovered before he left the company, and he later pleaded guilty under a plea bargain arrangement. [Ref. 6]

3. Compromised/Coerced Employees

A sailor with access to keys that has been caught by others, doing things that could be shameful and embarrassing, might be blackmailed into doing things he might not otherwise do. This could result in their compromise and exploitation by others without access to the network. As part of a security program, behaviors of a questionable nature must be taken into consideration.

4. Poorly Trained or Careless Users

Poorly trained personnel are not a normal threat. The problem here lies in accidentally destroying files, poorly designed passwords, or just doing something stupid that affects the network causing lost time and money. Deleted database files, important documents, even entire directories may be unwittingly deleted by someone with little computer experience. Poorly designed passwords are a problem that could allow someone easy access from the outside. Social engineering by outsiders to get login and password information is something that must be taught through training. Exposure of you system to users should be limited to only the privileges required to perform their job. If someone doesn't need access to a specific computer or certain files, then don't give them access. [Ref. 3]

5. Former Employees

Former employees, if not properly debriefed, may retain the ability to log onto their former network. They may have intimate knowledge of the system, user identifications, and passwords. As with the disgruntled employee, they may also bear a grudge against their former employer and seek retribution. Care must be taken to ensure that their ability to access the system is removed. Co-workers that may have shared information about their login and password should be reminded to change their passwords when a peer leaves the shop as well as warned about sharing changes to the information systems policies. [Ref 5]

6. Vendors and Contractors

Vendors and contractors present a unique threat. They are exceptionally familiar with the systems they install and maintain. However, they do not fall under the same guidelines as company employees. It is easy for a programmer from a vendor company to leave backdoors, which would allow them unlimited access to the system from a remote location. Employees of a vendor may cause more damage than your most untrustworthy user. Therefore it is wise to know the hiring and security practices of vendors with which you do business in order to reduce this threat. Closely monitor the activities of all vendors and contractors when they are on the site. A trusted employee should be with the vendor employee at all times while working on the system if possible. [Ref. 3]

C. EXAMPLES OF INSIDER ABUSE

The following examples of insider abuse show the seriousness of the insider threat: [Ref. 5]

In 1988, a Libyan intelligence agent obtained names, addresses and phone numbers of more than 1,000 federal employees at U. S. military and intelligence agencies. The information was obtained from his wife, who had access to the Metropolitan Washington Council of Governments listing for carpooling purposes through her job as a computer operator with the Virginia Department of Transportation. This was information that could have been used to assist in a terrorist operation.

Two Israelis associated with Israel's nuclear-weapons program illegally accessed a supercomputer at the Los Alamos National Laboratory's nuclear weapons facility in New Mexico. They used a friendly lab technician's access code and personal computer to connect into an unclassified but highly sophisticated Cray computer to work on designs for a nuclear-weapon detonator.

In 1993, the General Accounting Office determined that insiders posed the greatest threat to the National Crime Information Center. Fifty-six examples of intentional insider misuse was cited. Most of this misuse was relatively harmless use of information for personal purposes, for profit, or for political gain. In some cases, the misuse of information jeopardized the safety of citizens and potentially of law enforcement personnel. The most extreme example involved a former law enforcement officer who obtained information from three other officers and used it to track down and murder his girlfriend. Another case involved a female terminal operator conducting background searches for her boyfriend to determine whether or not clients of his drug operation were undercover agents.

According to a report of the Internal Revenue Service, as of 1993, 369 employees of the southwest region offices had been investigated or disciplined for using government computers to create fraudulent tax refunds or to browse through tax records of friends, relatives, neighbors and celebrities. One employee had altered approximately 200 accounts to receive kickbacks from bogus refund checks.

Social Security Administration officials revealed how insider accomplices assisted a West African credit card fraud ring by looking up records of credit card customers and providing the West Africans with additional identifying information to activate those cards. Twelve employees and three contract security guards were allegedly involved in selling the information for $10 to $50 per record. Officials believe that files on approximately 20,000 people have been accessed in this manner.

A fairly recent Los Angeles Times report by Ralph Vartabedian stated that low-level employees at federal payment centers embezzled money ranging from $11,000 to $3 million each by exploiting loopholes in the government's troubled accounting system.

All of these examples lead to one conclusion. The insider threat is real. Insiders already have access to your system and do not have the added burden of circumventing firewalls, routers, and proxy servers.

D. EXPLOITABLE VULNERABILITIES [Ref. 6]

The most widely exploited vulnerability by an insider is the lack of controls and checks to prevent him from removing sensitive documents, computers, or media from the work area. And the problem has increased over the past decade as exit checks have relaxed and restrictions in response to the easing of the Cold War tensions, reductions in manning, and increased employee use of portable and home computers. Employees usually have the ability to modify, manipulate, and delete data that they may access. Now they have the ability to email information via the Internet to anywhere in the world. Copying and physically removing information is virtually undetectable.

Employees with privileged access have the ability to cause the greatest harm and can do more than compromise information. Systems programmers may introduce malicious codes such as viruses, time bombs, or Trojan Horses. These could result in denial or disruption of service at predetermined times. Backdoors could be introduced for the exfiltration of information. Systems administrators could make nearly imperceptible changes to files, data, and access permissions as well as obvious changes such as denying access or taking control of the entire system. It is believed that the incorporation of commercial software into government information systems will only increase the risk of a vulnerability.

An insider with authorized access may use his inside status to launch attacks which could give him unauthorized access. Already existing inside a firewall reduces the hardship a hacker endures just to get inside a system. In the case of a military or government system, this access could be to Top Secret information that if released to foreign governments could cause grave damage to our national security—such as the recent Los Alamos Labs nuclear secrets release to the Chinese government.

An untrustworthy insider might be used to facilitate access to an outsider. The insider could be used to insert viruses for someone else. They may share passwords to remote login access. If they are good at snooping, they could easily find out passwords of peers and pass them along. Or something as simple as downloading known contaminated software could be accomplished.

Physical access to a system must be controlled. By allowing virtually unlimited access to systems throughout a company, or even a work center, this might allow an untrustworthy employee an advantage that is unnecessary. Many government jobs require different levels of access to systems. Control of access is essential to ensure that higher levels of access are not inadvertently given to lower level employees.

E. COUNTERMEASURES

1. Objectives [Ref. 6]

- Set limits and enforce them.
- Hold individuals accountable for their actions.
- Review audit logs religiously—more frequently for personnel with higher accesses.
- Make your system more resistant to sophisticated attacks by insiders.
- Use intrusion detection methods to detect access to sensitive information by unauthorized personnel.
- Perform damage assessments, localize damage, and recover in the event of a system security policy violation.

2. Access Control

The following are some of the most important characteristics that need to be addressed in order to implement effective technical access control:

- Access control criteria – a clear policy must be established and promulgated to all users to guide those managing accounts and granting access.
- Access control lists – provides a list at each workstation of all personnel authorized access.
- Access control tools – allows entry and maintenance of access control lists.

3. Identification and Authentication

In order to ensure that only authorized users gain access, you should use access-granting tools that will positively identify the user. This involves obtaining the users "claimed" identity followed by forcing the user to authenticate his identity. The simplest form of this is the typical login identification and password. Other forms include smart cards, retinal scanners, voice recognition, and signature recognition to name a few.

4. Encryption

After a user is authenticated and requests data, the unencrypted transmission may be intercepted by sniffers placed there by malicious insiders. Sensitive data transmitted on the network should be encrypted to prevent those without the need-to-know from intercepting and using in an unacceptable manner. Sensitive files should be encrypted as well to prevent someone from reading, even though they have gained access—no encryption key, no ability to read.

5. Operating System Controls and Administration Tools

The operating system plays a primary role in enforcing security policy and access control. Great care should be taken to ensure that all known holes are plugged and that appropriate settings are made to ensure security policies are enforced. Systems Administrators should be carefully selected and highly skilled. They are tasked with ensuring security policies are enforced and must be kept up-to-date in security information. For this reason, systems administration should be a full-time job and not an additional duty. Their knowledge should include the availability and use of network vulnerability scanner, such as SATAN, they aids in the discovery of holes in your system security.

6. Auditing and Logging

It is absolutely essential to keep logs of suspicious activities. Logging features of operating systems should be turned on and set to the highest level of performance possible without hindering operations too much. Audits on the logs should be performed regularly to search for suspicious activities. This is a manpower intensive job. Software packages exist today that will aid in this effort thus reducing the manpower needed and will compile profiles of individual usage patterns and behaviors on the network. These sophisticated packages will automatically scan large amounts of data and notify system monitors of suspicious activity.

7. Intrusion Detection

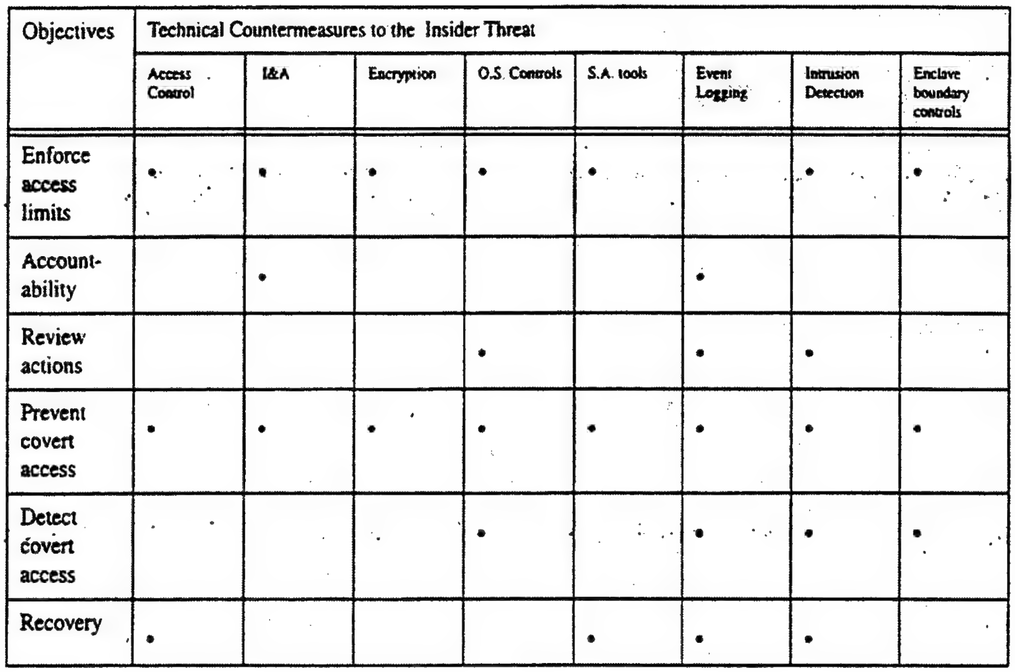
Intrusion detection packages monitor transactions at the network layer. The monitor events based on source and destination addresses and protocol types. These detection tools will identify signatures of known attack scenarios and behavior patterns.

Although designed as a backup to firewalls in the detection of intruders on the network, they will also double in the detection of suspicious activity by insiders as well. The best intrusion detection tools available can respond fast enough to shut down specific ports or the entire system in order to prevent further damage.

8. Firewalls

Firewalls normally prevent outsiders from intruding onto your networks. They may also be used within an organization to separate different departments thus adding in the protection of information from those without the need-to-know. These internal firewalls also aid in the prevention of spreading viruses within an organization.

The following table is provided as an aid to support objectives.



Objectives	Technical Countermeasures to the Insider Threat							
	Access Control	I&A	Encryption	O.S. Controls	S.A. tools	Event Logging	Intrusion Detection	Enclave boundary controls
Enforce access limits	•	•	•	•	•		•	•
Accountability		•				•		
Review actions				•		•	•	
Prevent covert access	•	•	•	•	•	•	•	•
Detect covert access				•		•	•	•
Recovery	•				•	•	•	

Table 3.1. Mechanisms to Support Objectives. From Ref. [6].

F. SUMMARY

Threats to computer systems can come for many sources. Chapter II discussed various external threats that can be costly to computer systems. However, the internal threat is just as real and can have a catastrophic effect on an organization. Insiders are legitimate computer users. They already have access to the organization's computer system and can use their knowledge to bypass security measures. The insider threat can come from many sources including; spies, disgruntled employees, comprised or coerced employees, former employees, or vendors/contractors. This threat is not limited to personnel who knowingly violate security measures; it can be an employee who has not been sufficiently trained in proper security protocol or simply a careless user. The lack of checks and controls provide an untrustworthy insider the freedom to remove sensitive information from networks. Many countermeasures have been developed that force the employee to follow the organization's computer security policy. Access control, identification and authentication, encryption, operating system controls, auditing, intrusion detection, and firewalls all provide some form of defense against an insider attack.

IV. PROFILING

A. WHAT IS PROFILING?

Profiling is the art of taking facts about an activity, storing these facts in a database, and attempting to gain some conclusions based on frequencies of occurrence to determine if an event is normal behavior or unexpected behavior within a particular context through the use of automated statistical analysis. The automated analysis is used to perform a check of audit logs. These audit logs can grow quite large and rapidly depending on the frequency with which events, within a network are logged.

B. USES

Profiling is used in a wide spectrum of applications domains.

1. Criminology

a. Racial

Racial profiling has gained a considerable amount of attention. There is much debate on whether this form of profiling actually exists or just appears to exist. It primarily concerns law enforcement officers detaining anyone based on the suspect's appearance. Why do this? It is difficult to ascertain if an individual is a criminal or not based on their skin color alone. However, there is a type of appearance that can lead one to believe a person might be a criminal or up to malicious mischief. Criminals are generally people that fail to adhere to a norm. Law-abiding citizens tend to dress as well as their social status will allow or better. They attempt to speak without using vile language in public, and they maintain a clean, fresh look such as a nice haircut and recently bathed. This is a norm that has been well established for many years. While it is true that someone may not be a criminal just because they are not well maintained in appearance, a sampling of a criminal population, especially criminals on the lower end of society, would reveal that many fit outside the norm. So is it fair to detain someone based on their appearance? That is up to the standards set by laws.

b. Investigative

There is no established date when profiling criminals first began, but the practice has been used for many years. Arthur Conan Doyle's Sherlock Holmes could profile someone with a glance. Today, behavioral specialists study similarities in criminal activity. They gather information about the criminal's early childhood, scholastic achievements, parental guidance, to name a few, in order to determine patterns in someone's past that might lead to a life of crime. Through gathering this information on the past of known criminals and developing statistics, it may be determined with some precision, if a person that has not yet committed a crime, may become a criminal in the future. This type of profiling is further carried out on the basis of the type of crime. Profiling is highly useful in tracking down serial criminals such as serial killers. The criminal's methods of killing, clues that may have been left behind (accidentally or intentionally), and information about the victims themselves may all be used to develop a profile on the criminal. If an accurate profile can be developed, this greatly aids in the capture and prosecution of the killer.

2. Meteorology

Dating back to the 1800's and perhaps earlier, weather data has been recorded. Today large databases hold various weather data such as temperature, wind speed and direction, precipitation, dew point, and humidity. Statistical analyses are performed to characterize nominal and extreme weather conditions.

Data is also collected from the ocean. The oceans, which cover over 70 percent of the earth's surface, greatly influence climates around the globe. Therefore it is important to study and understand the ocean and its influence on climate. Vertical profiling instruments play an important role in oceanography and are used to support the research in physical, chemical, and biological oceanography. The LEO-15 vertical profiler, operated by Rutgers University Institute of Marine and Coastal Science and deployed off the coast of New Jersey in 15 meters of water, includes sensors to measure chemical, optical, physical, and biological properties. As of 1997, its sensors are capable of measuring temperature, conductivity, pressure, dissolved oxygen, fluoride, transmissivity, optical backscatter, and photosynthetic active radiation. This data is stored and norms are determined. By monitoring this data, this system is aiding scientists in better understanding the coastal environment. These profiling systems greatly increase the ability of oceanographers to interpret oceanographic data which has been collected and stored. [Ref. 7]

3. Data Mining

Data mining has numerous applications. One such application deals with grocery stores. These stores issue discount cards. These discount cards, unbeknownst to many, are used to collect information on consumer buying habits. The consumer purchases groceries. As the groceries are tallied at the cash register, this information is stored in a computer. With the swipe of a card, the consumer's name is attached to the data. This information is sometimes sold to various companies that market other consumer goods.

The raw data is processed which develops a statistical profile of each individual. From this profile, companies determine which products a specific consumer will be most likely to buy, and tailor advertising and marketing promotions accordingly.

4. Example: Internet-Based Profiling

A form of data mining is also performed through the use of "cookies." A cookie is a few lines of information sent by a web server to store on a web browser so it can be retrieved from the browser later. Cookies are stored on the client machine and can only be deciphered by the server that set the cookie. Both Microsoft and Netscape web browsers use cookies to record user preferences for personal start pages. Cookies are used for online ordering systems, site personalization, web site tracking, target marketing, and user identification. Online ordering systems set cookies to remember what a person wants to buy, has bought, or is about to buy (what is in the "shopping cart"). For example, United Airlines uses cookies to store personal information about customers who make airline reservations via their web site. The cookie provides a convenient service to the customer because all the personal information is stored on the user's hard drive. The customer will not have to re-enter information the next time they return to the web site.

C. APPLICATIONS IN COMPUTER SECURITY

1. Software Profiling

Profiling does have some application in computer technology. One use of profiling is in memory management. An operating system attempts to determine which pages of a computer program are used the most. Then it will maintain these pages in RAM or cache for fast retrieval.

Another use can be found in the area of software development. Software reuse is the process of building new software systems from predefined software components. Recognizing this, an effort has been made to profile software components for reuse. One such effort has resulted in the Software Reuse System. [Ref. 8] This system consists of a storage module which classifies and stores software modules, and a retrieval mechanism that locates modules that programmers might want to use in a new project. The storage module constructs profiles, calculates similarity values using profiles and similarity functions, classifies software modules by the similarity values, and stores them.

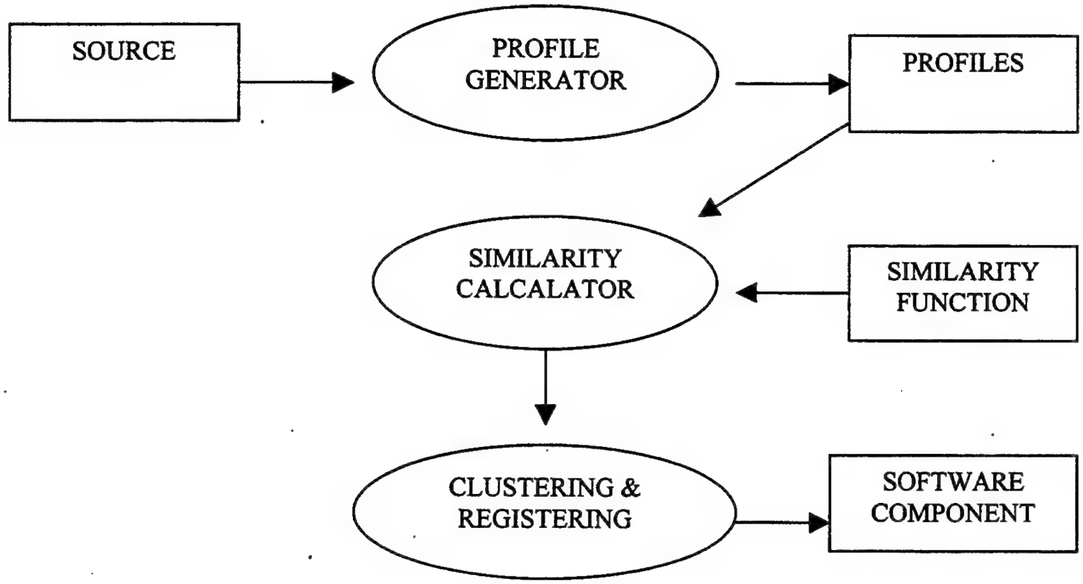


Figure 4.1. Storage Module of the Software Reuse System. After Ref. [8].

Two types of profiles are used in this process--Object Profiles and Virtual Profiles. The profile constructed from the software component is the Object Profile. A software component is scanned for information. The information obtained to produce a profile is the function name, function argument name, global variable name, local variable name, and comments. The Object Profile structure contains identifiers (of components, functions, and variables), weights (of function and variable identifiers), function pointer (which indicates the actual position of software components), and informal description (derived from comments embedded in source code).

Currently the jury is out on what affect profiling is having on the development of new software. However, it is believed that advances in software reuse via profiling will greatly enhance the ability of software developers to produce software at a more rapid pace than is possible without profiling. This in turn can lower the amount of resources that must be expended to develop software. The figure below shows the phases necessary to create a software reuse program.

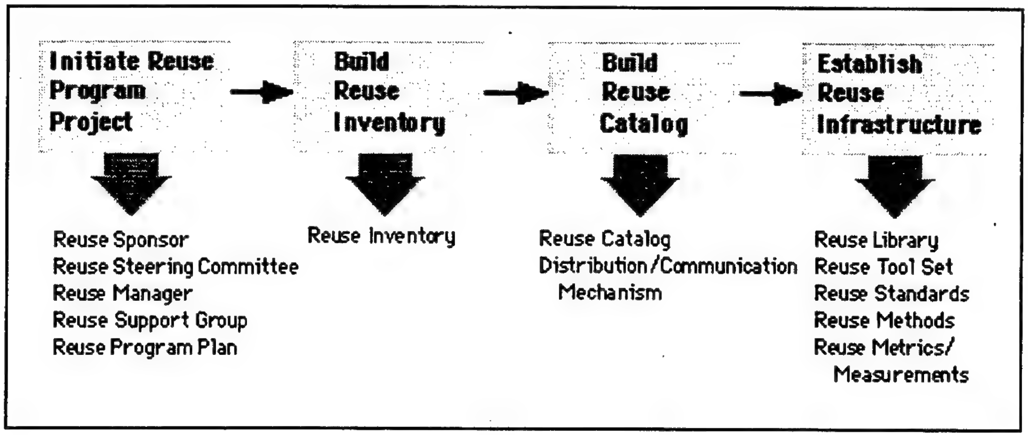


Figure 4.2. Phases of a *Reuse Program Creation* Project. From Ref. [9].

Since the beginning of programming, although it has been acknowledged as something that developers should do, software reuse has met with great resistance and frequent failure when attempted to put into actual practice across an organization. Why? The reasons why software reuse often fails to work in practice are just as obvious as the reasons why it is a good idea. Software developers and management have no difficulty citing a countless number of reasons such as:

- There is nothing to reuse.
- There is no management commitment or support.
- Reward and recognition programs are counter to reuse.
- Cost of reuse is too high.
- It is too time-consuming to find something to reuse and to understand it.
- Code reuse is more trouble then it is worth.
- Reuse is not a part of or even mentioned in current development methods.
- Current tools do not support reuse.
- Management is not convinced of the business value of reuse.
- Developers do not like reuse except it involves their own or perhaps their team members software.

Research on the topic of software reuse is ongoing. It is however, a current attempt to use profiling as a means to improve work.

2. Audit Reduction

Trusted systems must maintain audit trails of system activity in order that actions counter to policy may be traced back to the users of system resources. Even where foul play is not suspected, audit trails can be useful in restoring data integrity following innocent mistakes or failures of software. Unfortunately, if an audit trail is to be useful in tracing back an event after the fact, it must at all times record many system events at a fine level of detail. The result is a great volume of data, most of it uninteresting, which must be generated and stored in the hope that, if a suspicious event takes place, the few critical records will be present that are needed to trace the sequence of events leading up to a violation of security or other policy.

The sheer size of typical audit trails gives rise to two problems:

- The expense of storing audit trails can be significant, so space-efficient storage techniques must be developed.
- The audit trails must be processed somehow to provide security administrators with only the information of interest rather than mountains of data.

Because audit records can be generated rapidly in real time—depending on step-time, granularity of data, number of parameters, etc. The processing time required to address both problems must also be minimal.

The two problems are interrelated. Compression techniques applied to reduce storage expense may complicate the later processing of the trail. Conversely, the same techniques used to condense low-level detail into concise information for the security administrator can be used to reduce the information stored. This is a special example of a lossy compression technique, one where the loss can be explicitly tailored according to the needs of the security administrator.

A number of commercial-off-the-shelf products provide auditing capabilities and include tools for the reduction/abstraction of audit trails. However, the system designers generally make different decisions regarding what details should be recorded and application tools tend to be specific to those systems. Therefore care must be taken when choosing an audit reduction application to ensure it meets the needs of the system for which it is intended.

In deciding what details to record, designers take a calculated risk which is also inherent whenever details are condensed into higher-level records to save storage. The risk is that, when a suspicious event takes place, key details needed to reconstruct the event may not have been retained. Deciding what best to include in audit trails to minimize this risk is a goal of the Computer Operations, Audit, and Security Technology (COAST) Audit Trails Format Group (of Purdue University) and closely related to the work of this group.

The problem of processing audit trails automatically, to report only important sequences of events, encompasses audit reduction, misuse detection, and intrusion detection. To develop better and more general solutions requires reviewing multiple systems, and the effort to develop improved tools is most justified if the tools can be easily adapted to many systems. [Ref. 10] With distributed systems, a combination of hardware and software components are connected via a network. Varying software/hardware packages connected to a network may cause problems when attempting to monitor a system. The Computer Misuse Detection System, discussed in the next chapter, is capable of monitoring several different operating systems and hardware components.

3. Misuse/Intrusion Detection

Misuse detection involves real-time auditing and analysis capable of detecting and deterring computer misuse. Profiles are created over time for each user. A statistical analysis is also performed on a periodic basis to establish baselines against which to judge user behavior. By approximately 30 days, an average user should have developed a profile detailed enough to perform meaningful checks. Profiles are developed by processing large amounts of audit data. This data may be processed in real-time or, by batch method. Batch method is a means of checking the audit data automatically based on a schedule such as once per month or every seven days. Of course the ability to check the audit data at any time, "on demand," should be available to security personnel as well. The Computer Misuse Detection System, developed by Science Applications International Corporation (SAIC) and now marketed by ODS Networks, is just such a system and will be discussed in the next chapter.

Another system called Secure-IT 2000 provides security control and management of remote users wishing to access corporate networks via modems or ISDN. It monitors and analyzes all system access activity and generates a range of management reports from a comprehensive real-time event log and historical audit trails. Billing modules provide extremely accurate costs of all calls made to the system within 1 second.

With Secure-IT 2000, each user can be individually profiled for the type of access that is required such as: [Ref. 11]

- **Passthrough:** This option will allow the user, once authenticated, to passthrough to a host device.
- **Normal Dial-Back:** Once authenticated, the user will be called back at a set number from a modem or ISDN terminal adapter on a different telephone line. Up to three preset dial-back locations can be profiled per user.
- **Wild Dial-Back:** Once authenticated the user is allowed to enter a telephone number to which the system will make an outgoing call.
- **Temporary Users:** For temporary personnel such as contractors or consultants. This facility allows the administrator to enter the date at which the access rights of

a particular user will terminate. The system will automatically inhibit this user at midnight on that day.

- **Remote Console:** For support staff who need to gain administrative access to the master console. Once authenticated the technician is asked if he/she wants to connect as the master console.
- **Access Periods:** Each user is allocated his own access period timetable. The period is defined on a 7 day, 24 hour basis in blocks of 30 minutes.
- **Access Grouping:** Host ports can be configured into groups to form access points to different services, that is, Local Area Network Access Server, Unix Server, Terminal Server, etc. This means that user access to each individual host port or host service can be easily controlled.
- **Password Aging:** For users of user id, and password access, password aging can be enabled whereby the user is forced to change password after a set number of days up to a maximum of 99 days. The same password cannot be used for twelve occurrences of password changes.
- **User Class:** Each user can belong to one user class. This can then be used to group users together for reporting purposes. Up to 99 user classes can be defined.
- **Change Bands:** This option sets a defined charge class for a telephone number. This allows call costs to be calculated by the Secure-IT 2000 billing module. Up to 99 charge bands are definable.

D. MONITORS

Monitors are used to observe activities on a network. They observe performance, collect performance statistics, analyze data, and display results. Some reasons to monitor a system are: [Ref. 12]

- To find the frequently used segments of software and optimize performance.
- Measure resource utilization and locate performance bottlenecks.
- Tune a system/network.
- Characterize the workload and use this information for capacity planning and creating test workloads.
- Find model parameters, validate models, and develop inputs for models.

Monitors are classified in several ways but three primary classifications are: 1) hardware, 2) software, and 3) firmware. We will concentrate primarily on hardware and software monitors.

1. Software Monitors

Monitoring operating systems, database management systems, networks, and applications can be accomplished with software monitors. However, these monitors are suitable only if the input rate is low. Input rate is the maximum frequency of events that a monitor can correctly observe. Due to the monitor being a software program that is running on the systems being monitored, the system may lose some speed. They generally have lower input rates, lower resolutions, and higher overhead than hardware monitors.

2. Hardware Monitors

A hardware monitor is made up of separate pieces of equipment that are attached to a system via probes. Virtually no resources of the system being monitored are used by a hardware monitor as it only senses, via probes. The probability of introducing bugs into the system is generally lower that for software monitors. These hardware monitors consist of the following elements: [Ref. 12]

- Probes – used to observe signals at desired points in the system hardware.
- Counters – incremented whenever a particular event occurs.
- Logic Elements – Signals from many probes can be combined using AND, OR, and other logic gates. Combinations are used to indicate events that may increment the counters.
- Comparators – can be used to compare counters or signal values with preset values.
- Mapping Hardware – allows histograms of observed quantities to be computed. Consists of multiple comparators and counters.
- Timer – used for time stamping or for triggering a sampling operation.
- Tape/Disk – for storage of collected data.

3. Hardware Versus Software

Should a hardware monitor or a software monitor be used? Several factors should be considered. The first step in making such a decision is to consider what needs to be measured. Hardware monitors can sense electrical signals on the busses and can accurately record them. But it is difficult for these monitors to detect higher level information such as queue lengths or current number of users unless the information is stored in a hardware register. On the other hand, software monitors can easily determine the higher level information but cannot observe low-level events. Other considerations are listed in the following table:

Criterion	Hardware Monitor	Software Monitor
Domain	Difficult to monitor operating system events.	Difficult to monitor hardware events unless recognizable by an instruction.
Input Rate	Sampling rates of 10^5 per second possible.	Sampling rate limited by the processor MIPS and overhead required.
Time Resolution	10 nanoseconds is possible.	Generally 10 to 16 milliseconds.
Expertise	Requires intimate knowledge of hardware.	Requires intimate knowledge of software.
Recording capacity	Limited by memory and secondary storage.	Limited by overhead desired.
Input width	Can record several simultaneous events	Cannot record several simultaneous events unless there are multiple processors.
Monitor overhead	None	Overhead depends upon the input rate and input width.
Portability	Generally portable.	Specific to an operating system.
Availability	Monitoring continues even during system malfunction or failure.	Cannot monitor during system crashes.
Errors	Possible to connect the probes to wrong points.	Once debugged, errors are rare.
Cost	High	Medium

Table 4.1. Comparison of Hardware and Software Monitors. From Ref. [12].

4. Distributed-System Monitors

The majority of computer systems today are distributed and consist of many hardware and software components the work together separately and concurrently. It is more difficult to monitor distributed systems than it is to monitor centralized systems. The monitor itself must be distributed and should consist of several components that work separately and concurrently. Several layers make up these monitors. These layers are: [Ref. 12]

- Observation – gathers raw data on individual components of the system.
- Collection – collects the data from the observers.
- Analysis – analyzes the data gathered by the collectors.
- Presentation – this component provides the human interface and produces reports, displays, and alarms.
- Interpretation – the intelligent entity (human or expert system) that can make meaningful interpretations of the data.

The console provides an interface to control the system parameters and states, while the management module makes the decision to set or change system parameters or configurations based on interpretation of monitored performance.

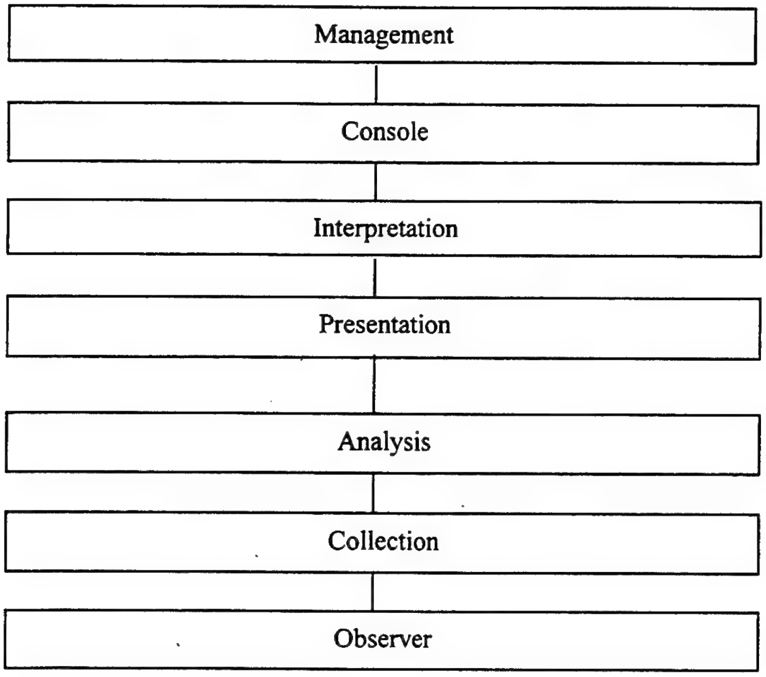


Figure 4.3. Layered View of a Distributed-System Monitor. From Ref. [12].

In the next chapter, we describe the Computer Misuse Detection System (CMDS). CMDS has all the capabilities of a distributed system monitor.

E. SUMMARY

Profiling is not new, and has been used in many fields other than computer security management. Criminology, meteorology, and data mining all use some form of profiling to accomplish specific goals.

Profiling is the art of determining a unique set of characteristics that identify a type or category of person. In the computer security field, profiling is an electronic way of determining the normal behavior of a user from statistical data. Once this data is obtained, a normalized pattern of behavior can be produced. The user's current activity is then compared to the normal behavior to determine if any unusual activity has occurred. Some specific applications are memory management, audit reduction, and intrusion detection. Additionally, monitors are used to observe activities on a network. The three primary classifications of monitors are software, hardware, and firmware.

THIS PAGE INTENTIONALLY LEFT BLANK

V. COMPUTER MISUSE DETECTION SYSTEM

A. INTRODUCTION

The commercial product Computer Misuse Detection System (CMDS) is intended to help provide an integrated Information Security management strategy. [Ref. 13] An integrated security plan consists of a set of enforcement policies, which define in detail the plan, strategy, and tactics for each security situation. These policies may define different stances for the same situation for sub-organizations or individual roles within an overall plan, such as a Command Security Policy. The Information Security manager must define a security stance that balances the need to maintain organizational security, with the need for access as well as legal and political constraints.

CMDS performs analyses of computer system audit data and ancillary data to automate the computer misuse detection process in networked data processing environments. It detects security-relevant events that may constitute evidence of attacks against information stored on, processed on, or transmitted by computers. The strength of CMDS is that it can gather and process audit log information from many platforms in a timely manner and present it in an organized easy-to-use format. Its goal is to provide the capability to process a wide range of security policies in an effective manner.

Networked computer environments consist of hardware platforms and software operating systems and applications from a diverse set of manufacturers. Many operating systems and software applications are capable of producing some form of audit information. This information normally has little consistency in format from one source to the next. In addition, audit data collection tends to operate at a low level of data abstraction. This results in tremendous amounts of data being collected, which are impractical to analyze using manual methods. Depending on the level of auditing that is enabled, a software package may be capable of capturing a level of detail almost down to a keystroke.

Additionally, making sense of audit information may require access to ancillary data sources outside of the audit data trail, such as mapping of IP addresses to host names, or user ID's and platforms to user names. The format of audit information may also be very diverse consisting of a variety of ASCII file formats or binary formats such as array or database formats.

CMDS provides a tailored set of processing engines to reduce the analysis effort, and an advanced GUI interface for reporting, status, and configuration.

The process of detecting security-relevant events is dependent on having a knowledge of the patterns of evidence which constitute the events. A defined pattern of evidence is called an event signature. Event detection is a pattern matching process. Sequence-dependent events may require multiple passes through the data for complete signature identification.

The use of multiple methods, or engines, for signature detection presents some data management problems in a distributed environment. It is advantageous to standardize data as early in the process as possible, so that the minimum number of passes can be made for signature detection, and engines can be generalized. CMDS events are of two basic types - primary and derived. Primary events can be obtained solely by reference to a single entry in the original audit source. Derived events are obtained by applying more complex process rules to primary events. These events may be entered into the database either by updating fields in pre-existing Event Record, or by creating a new Event Record based on rules applied from a variety of sequential processing engines.

All CMDS events are derived from some form of audit evidence. In other words, they can be mapped back to primary data obtained from the original audit source(s), or from a combination of audit source information, local information, or historical profile (statistical) data.

B. HOW CMDS WORKS?

CMDS is based on a "client-server" architecture. It reads audit data from client machines (called "targets" or "agents") and sends the information to the server machine to help detect deviations from expected behavior, adherence to predefined threat behavior, and suspicious trends in all system activity. [Ref. 13]

The CMDS server collects and reduces large numbers of audit records on heterogeneous networks. (Figure 5.1 provide an example of CMDS running on a heterogeneous network.) An audit record consists of sequential, discrete data elements that indicate an action has taken place. It gathers data from any supported target audit data source through a target daemon where the data is parsed into a common format, buffered, encrypted, and transported in near real-time to a server running on the CMDS server workstation.

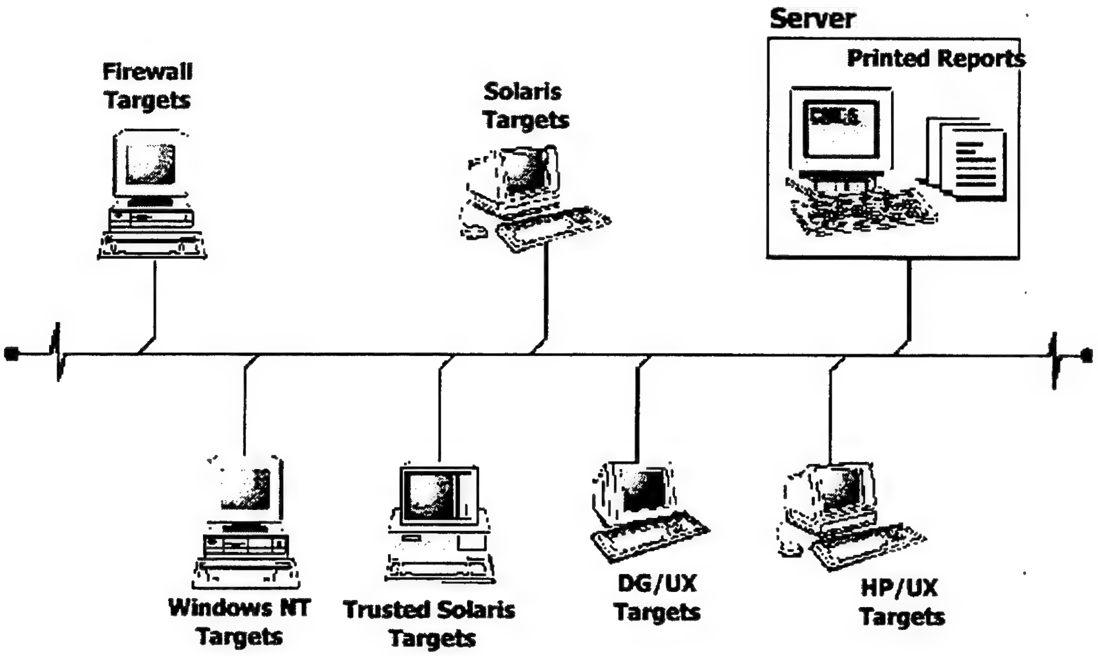


Figure 5.1. CMDS Operating on a Heterogeneous Network. From Ref. [13].

CMDS processes data in three different modes: Real-Time, Batch, and On-Demand.

- **Real-Time**: Audit records are processed as they are created at the target source. See Figure 5.2.
- **Batch:** Audit records are processed at per-specified times in groups (files).
- **On Demand:** One audit record is processed at the request of the operator.

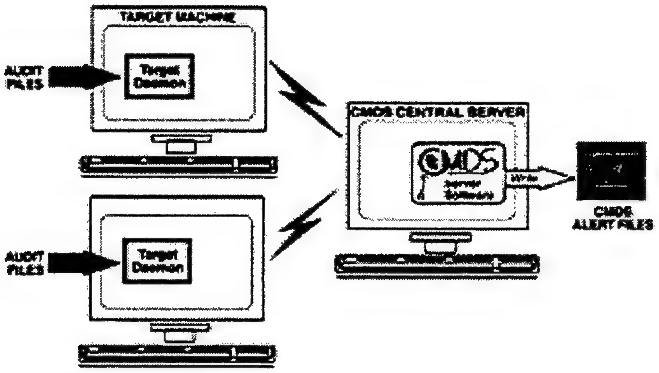


Figure 5.2. Real-Time Processing. From Ref. [13].

1. Real-Time Processing

The target daemon runs continuously on each target in the real-time environment. It reads the current audit files and sends the audit data to the real-time server. The data is then sent from the target daemon to the server in buffers of 5 to 999 records. [Ref. 13]

2. Batch Processing

This mode is used to reduce network overhead during peak hours of operation, or if you need to isolate the CMDS Server machine from the rest of the network. Audit files are sent from the target machine to the server machine's batch processing area on a periodic basis.

3. On-Demand Processing

This mode provides a special type of audit data processing. It enables the user to select a specific audit file to be processed individually. Typically, it would be used to process a data file that was created before CMDS was installed; to reprocess a data file, possibly with new configuration parameters; or for targets that do not have a direct connection to the CMDS server machine.

4. Server Operation

The server software reduces data through statistical and rule-based methods and outputs both real-time alerts and graphical reports. [Ref. 13] It uses attack signatures, statistical profiling, and graphical summaries to assist in detection. Figure 5.3 displays a CMDS system overview.

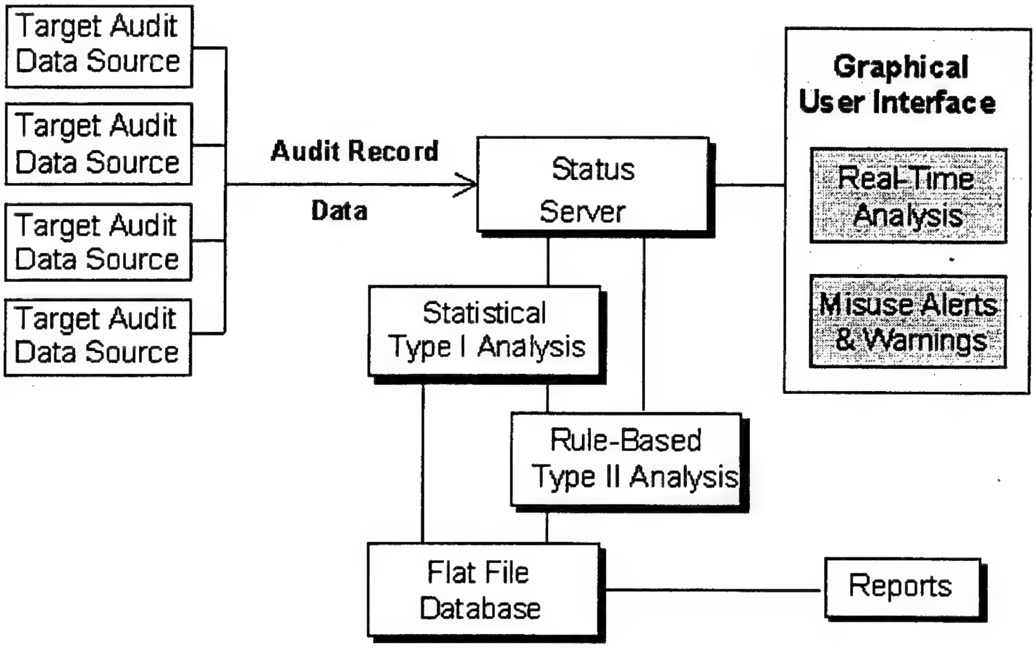
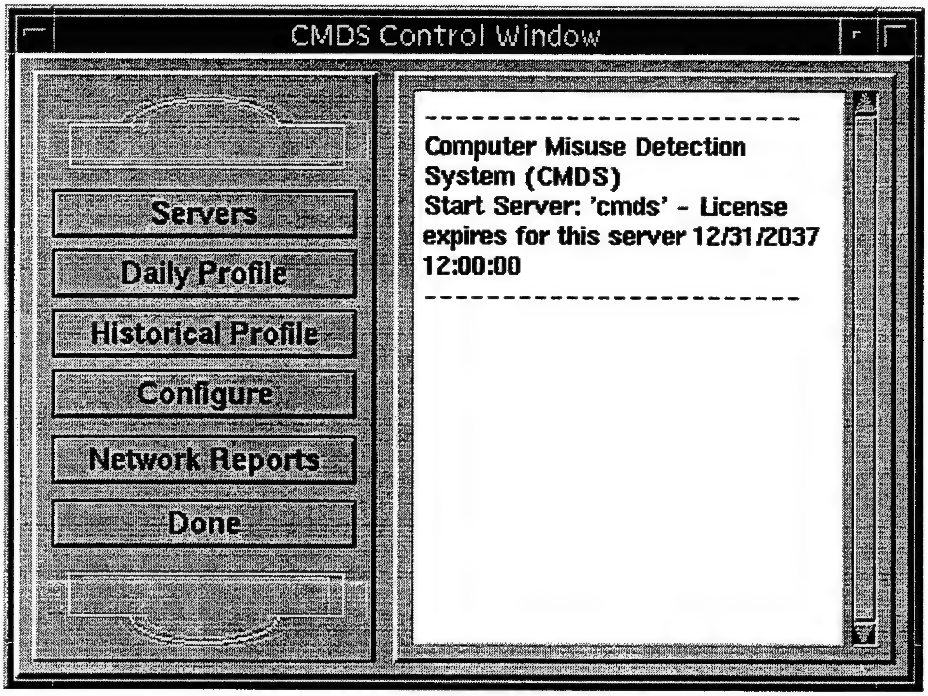


Figure 5.3. Sample CMDS System Overview. From Ref. [13].

Computer audit records are generated from a number of sources including operating system audits, application audits, database audits, and network management audits. CMDS uses audit records from the operating system and firewalls. Typically, all audit records, regardless of source, contain an event number user identification, time stamp, and object (filename). CMDS uses this information to create its own unique audit record format from records gathered across many target audit sources.

C. GRAPHICAL USER INTERFACE

CMDS incorporates a Motif-based graphical user interface (GUI) that provides a user-friendly interface. Once CMDS is properly configured, a user can perform almost all of the program's operations through these GUIs. The Control Window (Figure 5.4), appears on the screen after CMDS is started and provides access to most of the functions and operations needed.

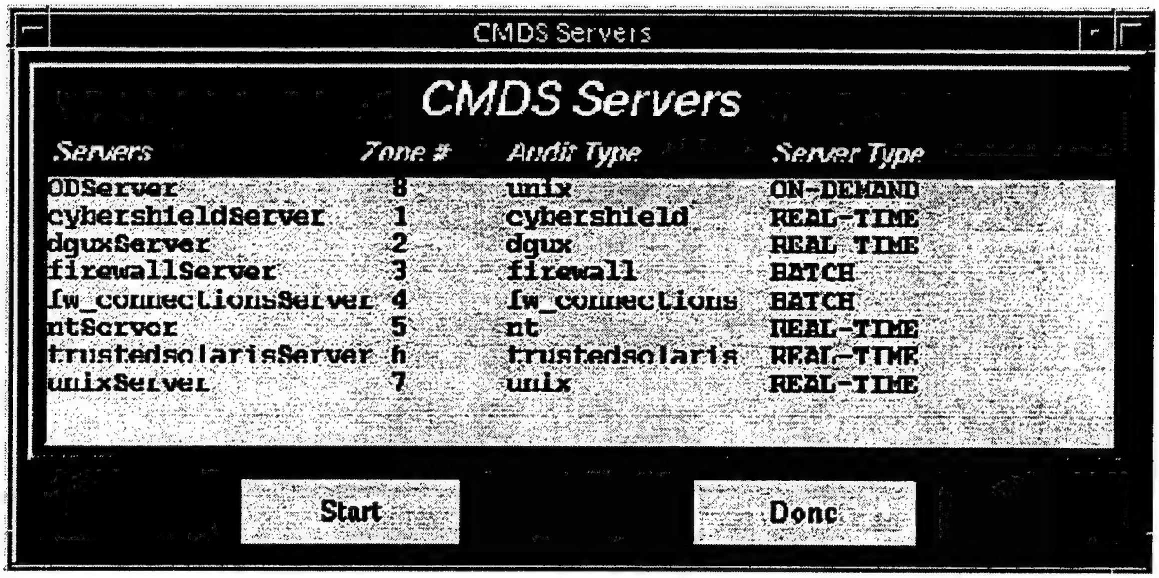


```
------------------------
Computer Misuse Detection
System (CMDS)
Start Server: 'cmds' - License
expires for this server 12/31/2037
12:00:00
------------------------
```

Figure 5.4. CMDS Control Window. From Ref. [13].

1. Starting CMDS Servers

This section describes how to start and use CMDS Servers to process data from single or multiple servers.



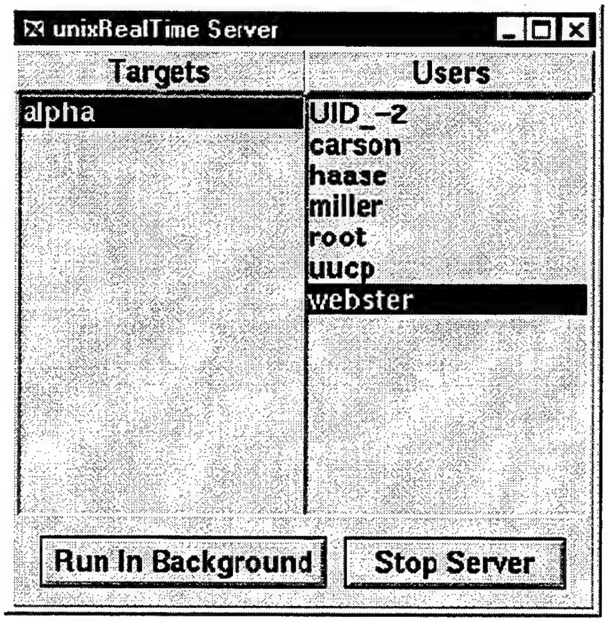
Servers	Zone #	Audit Type	Server Type
ODServer	8	unix	ON-DEMAND
cybershieldServer	1	cybershield	REAL-TIME
dguxServer	2	dgux	REAL-TIME
firewallServer	3	firewall	BATCH
fw_connectionsServer	4	fw_connections	BATCH
ntServer	5	nt	REAL-TIME
trustedsolarisServer	6	trustedsolaris	REAL-TIME
unixServer	7	unix	REAL-TIME

Figure 5.5. The CMDS Servers Window. From Ref. [13].

To gain access to the CMDS Servers window, click on the Servers button on the CMDS Control Window. The CMDS Servers window, shown in Figure 5.5 will appear on your screen. The following information is contained on the Servers window: [Ref. 13]

- **Servers:** Lists the name of each CMDS server that is configured to start.
- **Zone #:** This is a unique number in which CMDS identifies each server. The target daemon uses the zone number to know with which server to connect.
- **Audit Type:** Lists the audit type.
- **Server Type:** REAL-TIME, BATCH, or ON-DEMAND.
- **Start:** Starts the server you have selected.
- **Done:** Closes the CMDS Servers window.

To begin, select the CMDS server or servers you want to start then click on the Start button to bring up the Server Control and Alert List windows. The Starting server <server name> message will appear. For each server you select, a Server Control window and an Alert List window will appear. Figure 5.6 shows the Server Control window. When a target daemon begins collecting audit data for the server, the names of targets being monitored appear in the left-hand column of this window. The target name will blink to indicate that the CMDS server is currently receiving data from that particular target.

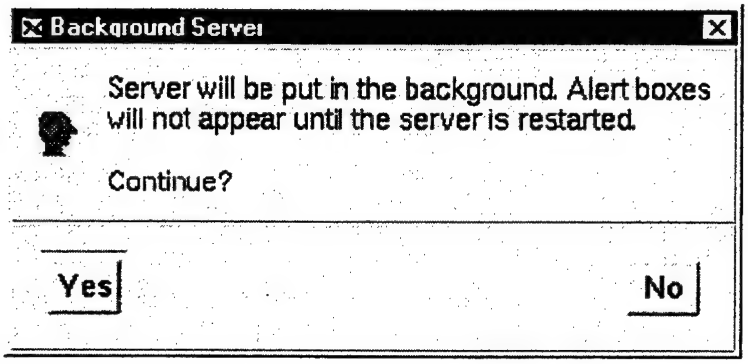


Targets	Users
alpha	UID_-2 carson haase miller root uucp webster

Figure 5.6. The Server Control Window. From Ref. [13].

To view a list of users for a particular target, click on the target name. A user list for that target will appear in the right-hand column.

To use the Guiless Server feature, click on the Run In Background button. A dialog box (Figure 5.7) will appear asking if you want to put the Server in the background. In Guiless Server mode, alert and warning boxes are not displayed, but alert and warning information is stored for future retrieval.



Server will be put in the background. Alert boxes will not appear until the server is restarted.

Continue?

Figure 5.7. The Background Server Dialog Box. From Ref. [13].

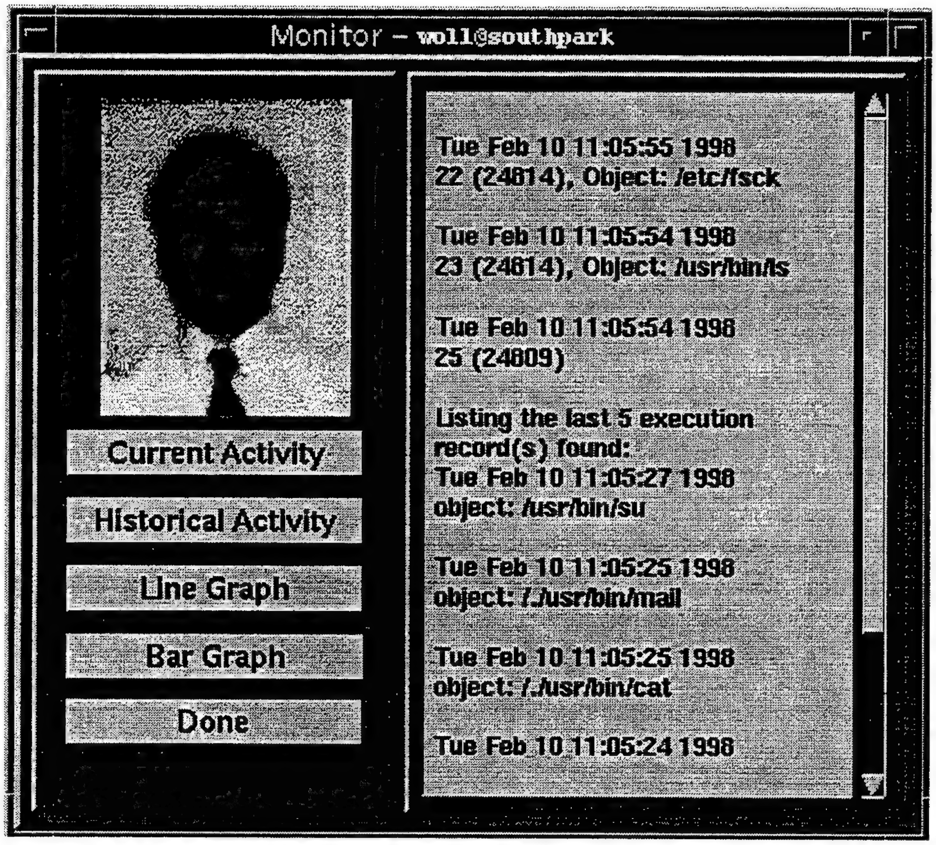
Select the Stop Server button to stop the server and close the Server Control window. [Ref. 13]

2. Real-Time Servers

Real-time servers are used to monitor critical targets in a timely manner. From the Server Control window, follow these steps to access the Monitor window:

Select the target name to view the users associated with a specific target. The users field contains names of users who have had an audit record created with their user ID since midnight of the current day. [Ref. 13]

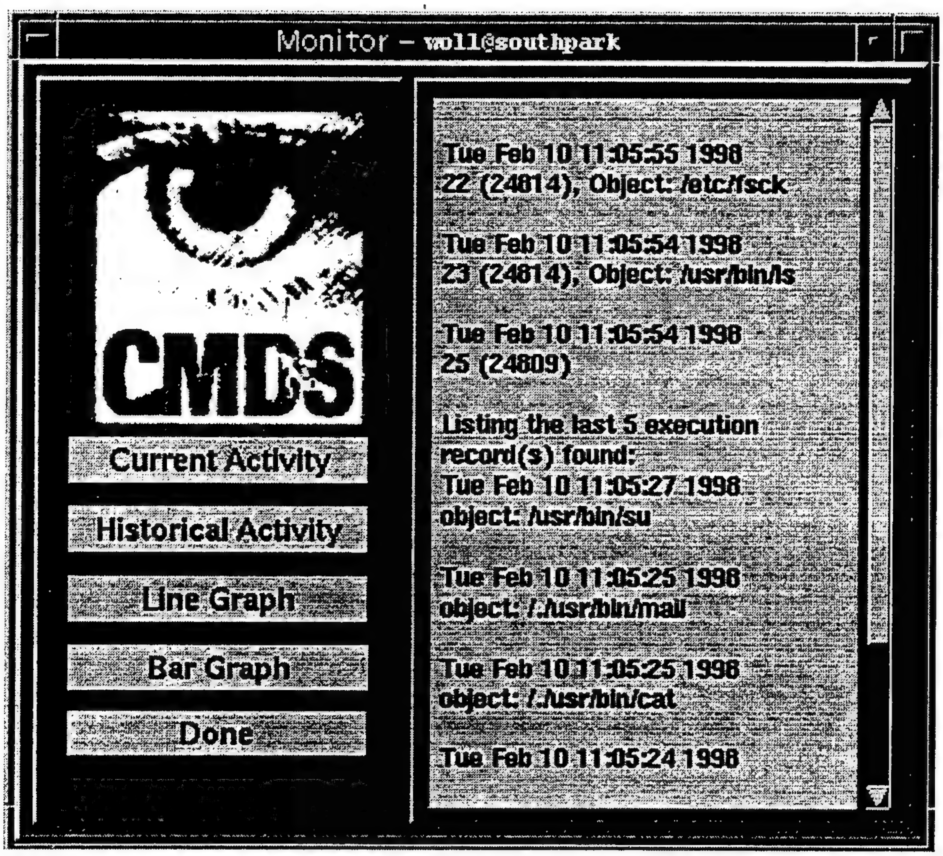
Select the user's name to obtain information about his or her activity during the current session or during the historical data period. The Monitor window will appear as shown in Figure 5.8 and Figure 5.9. You can view multiple Monitor windows simultaneously by selecting the names of users whose activity you want to monitor.



```
Tue Feb 10 11:05:55 1998
22 (24814), Object: /etc/fsck

Tue Feb 10 11:05:54 1998
23 (24814), Object: /usr/bin/ls

Tue Feb 10 11:05:54 1998
25 (24809)

Listing the last 5 execution
record(s) found:
Tue Feb 10 11:05:27 1998
object: /usr/bin/su

Tue Feb 10 11:05:25 1998
object: /./usr/bin/mail

Tue Feb 10 11:05:25 1998
object: /./usr/bin/cat

Tue Feb 10 11:05:24 1998
```

Figure 5.8. The Monitor Window. From Ref. [13].

Each Monitor window displays an image of the user along with raw audit data the user is currently generating. You can scan user images into the computer and store them in the CMDS_DIR/images file in .gif format. The .gif file name needs to be the same as the user name in order for the image to appear correctly. If the user's image is not available, the CMDS default image appears, as in Figure 5.9.



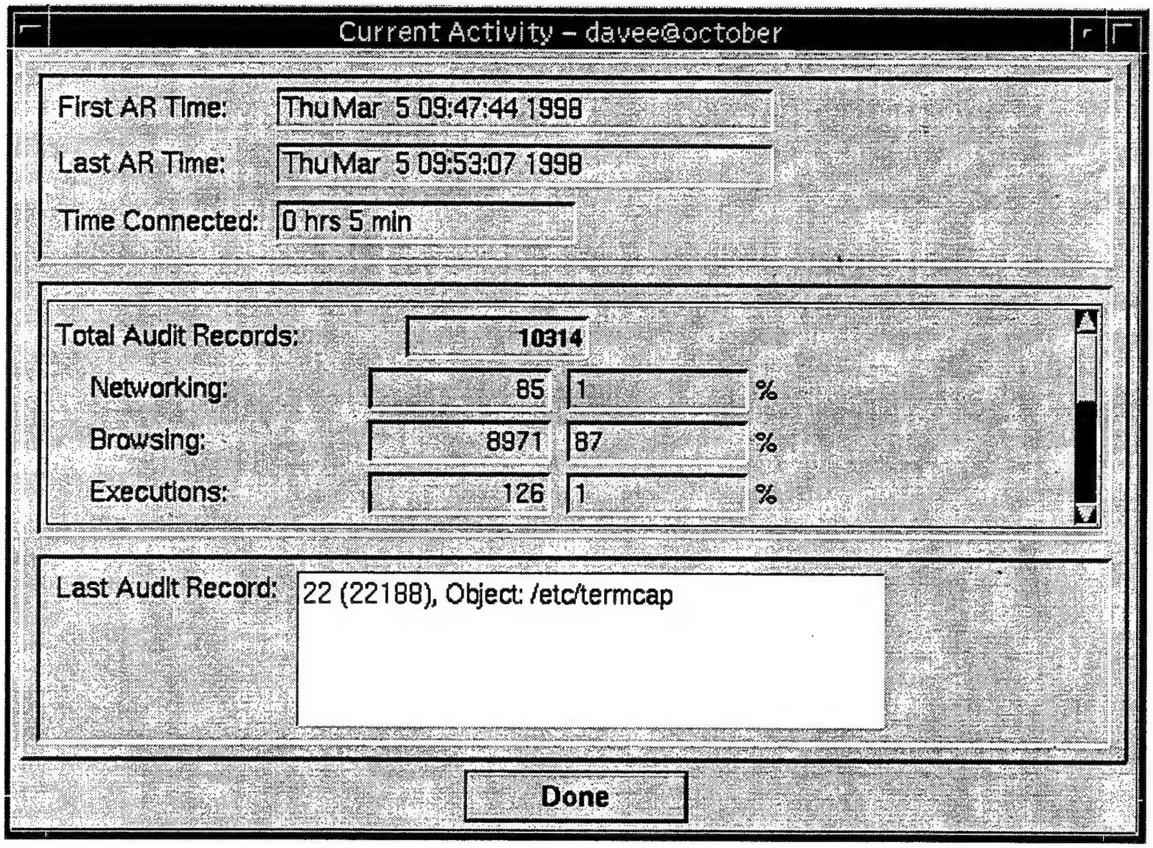
```
Tue Feb 10 11:05:55 1998
22 (24814), Object: /etc/fsck

Tue Feb 10 11:05:54 1998
23 (24814), Object: /usr/bin/ls

Tue Feb 10 11:05:54 1998
25 (24809)

Listing the last 5 execution
record(s) found:
Tue Feb 10 11:05:27 1998
object: /usr/bin/su

Tue Feb 10 11:05:25 1998
object: /./usr/bin/mail

Tue Feb 10 11:05:25 1998
object: /./usr/bin/cat

Tue Feb 10 11:05:24 1998
```

Figure 5.9. The Monitor Window with the Default Image. From Ref. [13].

The five options (Current Activity, Historical Activity, Line Graph, Bar Graph, Done) and the corresponding windows are discussed in the following sections.

a. Current Activity Window

The Current Activity window, shown in Figure 5.10, provides a real-time statistical representation of the user's behavior during the current session. The caption header displays the user (davee) and the hostname (october). The current session begins with the first record generated after midnight and ends the following midnight.



Current Activity – davee@october

First AR Time: Thu Mar 5 09:47:44 1998

Last AR Time: Thu Mar 5 09:53:07 1998

Time Connected: 0 hrs 5 min

Total Audit Records: 10314

Networking:	85	1	%
Browsing:	8971	87	%
Executions:	126	1	%

Last Audit Record: 22 (22188), Object: /etc/termcap

Figure 5.10. The Current Activity Window. From Ref. [13].

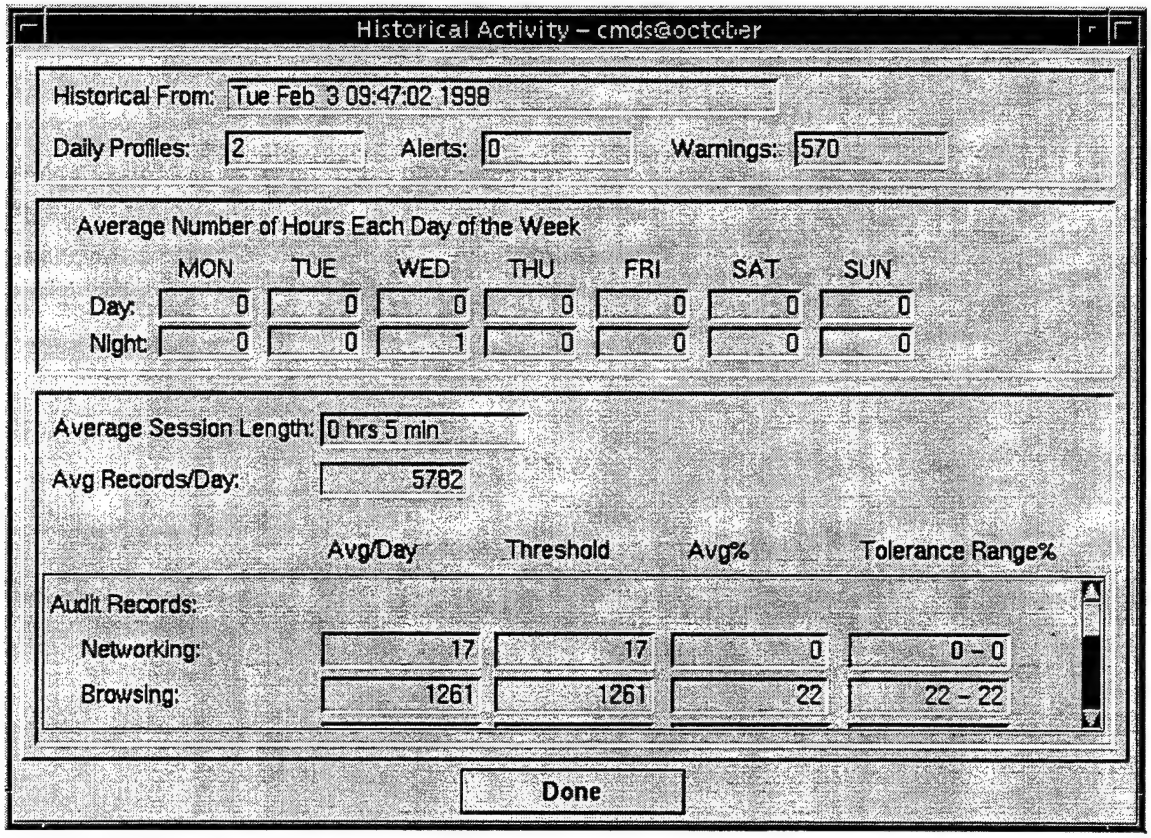
The Current Activity window displays the following data: [Ref. 13]

- **First AR Time:** The date and time the user generated the first audit record after midnight.
- **Last AR Time:** The last time the user generated an audit record up to and including midnight.
- **Time Connected:** The amount of time in hours and minutes the user has been active during the current session. This is the amount of time between First AR Time and Last AR Time.

- **Total Audit Records**: The number of audit records the user has generated since midnight.
- **Category Audit Records:** The number of audit records generated in each statistical category, and the percentage of these records versus the total number of records generated during the current session.
- **Last Audit Record:** The last CMDS (normalized) event number, the process ID (in parenthesis), and the object. The object is the last audit record found.
- **Done:** Closes the Current Activity window.

b. Historical Activity Window

The Historical Activity window, shown in Figure 5.11, provides statistical information when data for more than one day is found. The default historical data period is 90 sequential days, which includes the day before the current date. The user has the ability to configure this time period.



Historical From: Tue Feb 3 09:47:02 1998

Daily Profiles: 2 Alerts: 0 Warnings: 570

Average Number of Hours Each Day of the Week

	MON	TUE	WED	THU	FRI	SAT	SUN
Day:	0	0	0	0	0	0	0
Night:	0	0	1	0	0	0	0

Average Session Length: 0 hrs 5 min

Avg Records/Day: 5782

	Avg/Day	Threshold	Avg%	Tolerance Range%
Audit Records:				
Networking:	17	17	0	0 – 0
Browsing:	1261	1261	22	22 – 22

Figure 5.11. The Historical Activity Window. From Ref. [13].

The Historical Activity window displays the following data: [Ref. 13]

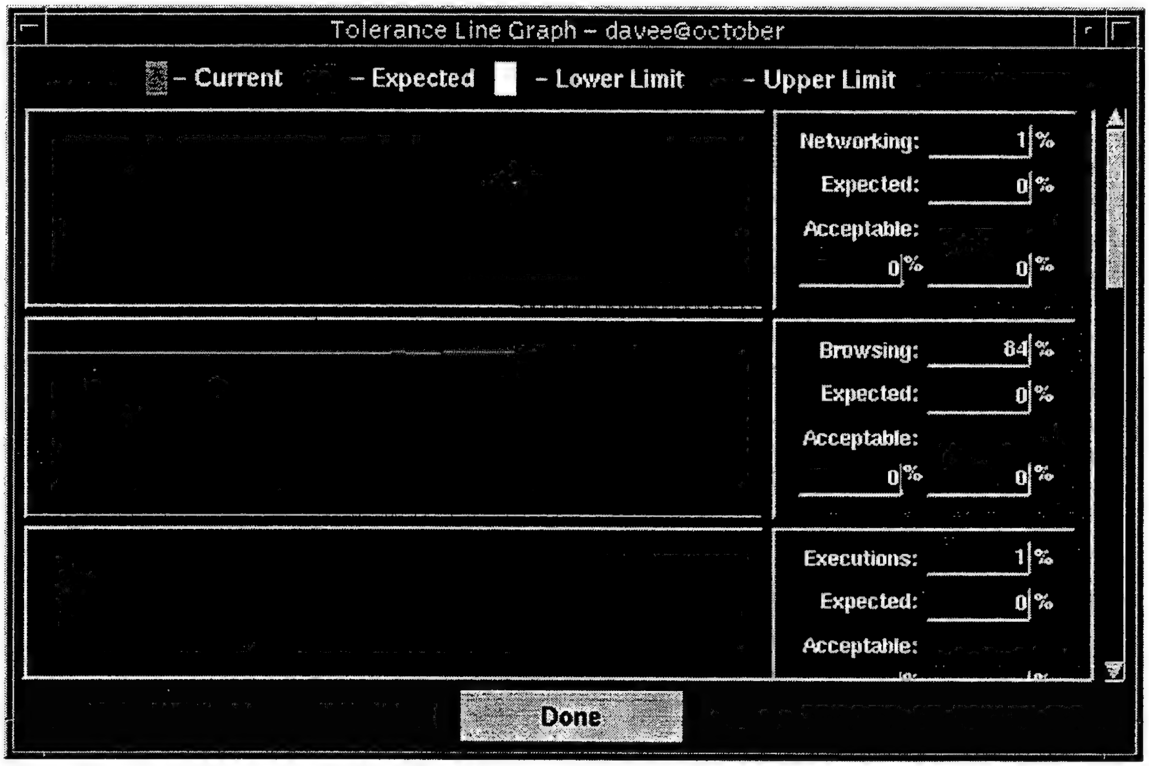
- **Historical From:** The start date and time of the historical data period.
- **Daily Profiles:** The number of days the user cmds@october has been logged in during the historical data period.
- **Alerts:** The number of alerts generated by the user cmds@october during the historical data period.
- **Warnings:** The number of warnings generated by the user cmds@october during the historical data period.

- **Average Number of Hours Each Day of the Week:** The average number of hours of user activity during the day and night for each day of the week during the historical period. This time is calculated by taking the average between the First AR Time and the Last AR Time for each day.
- **Average Session Length:** The average length of the user's sessions during the historical data period. This is a calculation of the time between First AR Time and Last AR Time.
- **Avg Records/Day:** The average number of audit records generated for each day cmds@october had activity during the historical data period.
- **Audit Records:** Contains a scrollable list of the statistical category audit records. Read across for average, threshold, percentage, and tolerance range statistics for each statistical category.
- **Avg/Day:** This field displays, for each statistical category, the average number of audit records generated for each day the user is logged in during the historical data period.
- **Threshold:** This field displays, for each statistical category, the threshold, which is the average per day plus the standard deviation of the historical data period.
- **Avg%:** This field displays, for each statistical category, the average percentage of records in the historical data period.
- **Tolerance Range%:** This field displays, for each statistical category, the percentage range, which is the average percentage of plus and minus the standard deviation percentage of the historical data period.

- **Done:** Closes the Historical Activity window.

c. *Tolerance Line Graph Window*

The Tolerance Line Graph window, shown in Figure 5.12, provides a real-time statistical representation of the deviation of current behavior from historical behavior in line graph form for each category of audit record generated. The name of the user and target appears at the top of the window.



Networking: 1 %
Expected: 0 %
Acceptable:
0 % 0 %

Browsing: 84 %
Expected: 0 %
Acceptable:
0 % 0 %

Executions: 1 %
Expected: 0 %
Acceptable:

Figure 5.12. The Tolerance Line Graph Window. From Ref. [13].

The Tolerance Line Graph window displays the following data for each statistical category: [Ref. 13]

- **Lines:** The solid aquamarine line shows data from the current session, in real time. The solid green line shows the expected percentage of category audit records generated. The broken red and yellow lines show the expected percentage plus and minus the standard deviation. Red indicates the upper limit, and yellow indicates the lower limit of the expected values.

- **Percentages:** The Tolerance Line Graph window displays the following for each statistical category.
- **Statistical category:** The percentage of audit records, by specific category, generated during the current session.
- **Expected:** The mean percentage of audit records, by specific category, generated from the user's historical data.
- **Acceptable:** Lists the range of percentage of audit records, by specific category, generated from the user's historical data.
- **Done:** Closes the Tolerance Line Graph window.

d. Behavior Bar Graph Window

The Behavior Bar Graph window, shown in Figure 5.13, provides a real-time representation of the number of audit records in a category as part of the total number of audit records generated during the current session.

- **Bars:**
  1. The green bar shows the number of statistical category audit records generated on the current day.
  2. The blue bar shows the average number of statistical category audit records generated per day.
  3. The orange bar shows the threshold number of statistical category audit records.

4. The green bar turns red when the number of statistical category audit records has exceeded the threshold.

- **Numbers:** The Behavior Bar Graph window shows the following data for each statistical category:
- **Above the green bar:** The number of audit records found.
- **Below the orange bar:** The threshold value. CMDS places the threshold value for each category two-thirds of the distance along the bar. Notice that each statistical category bar has its own scale, depending on its threshold value.
- **Done:** Closes the Behavior Bar Graph window.

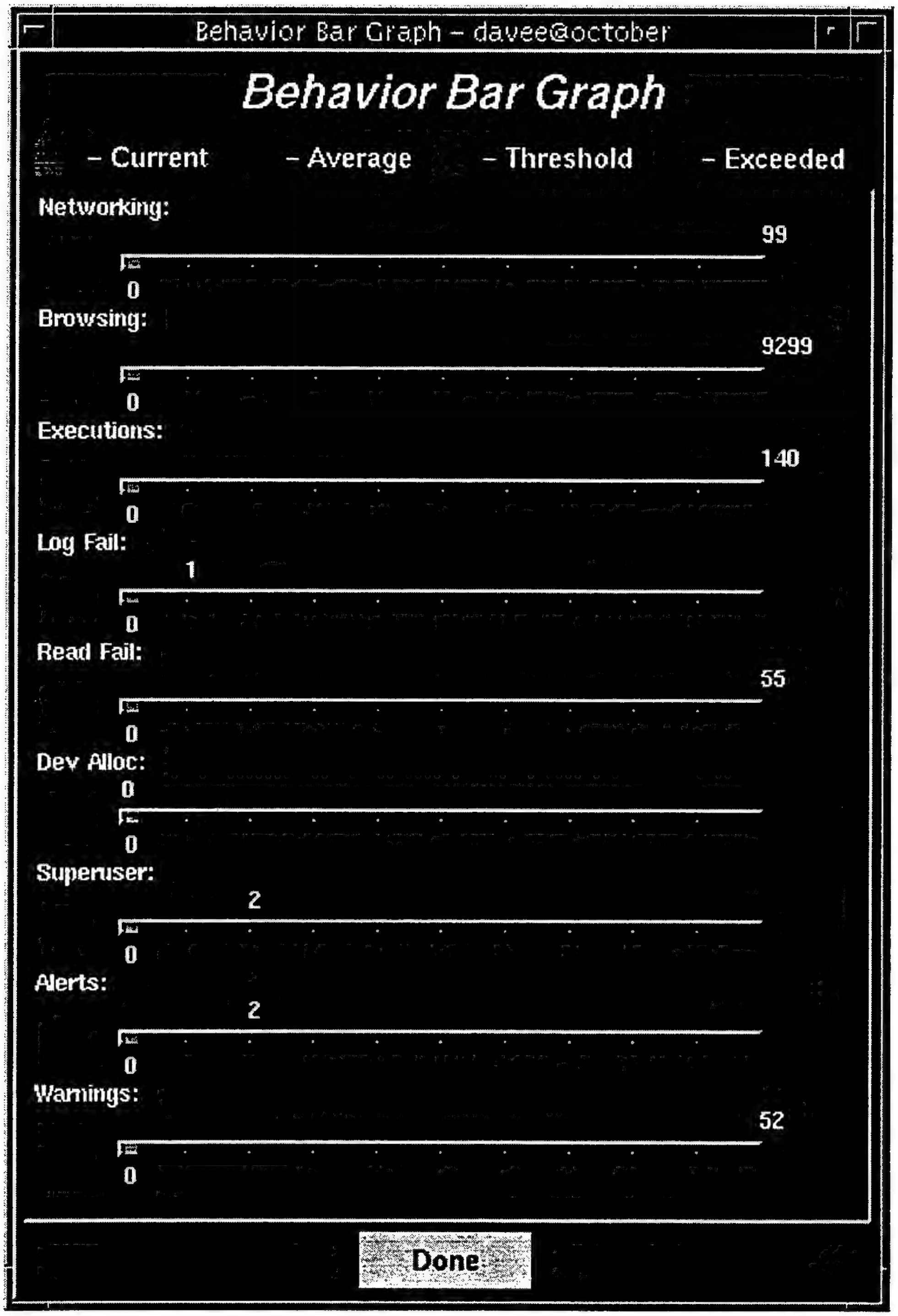
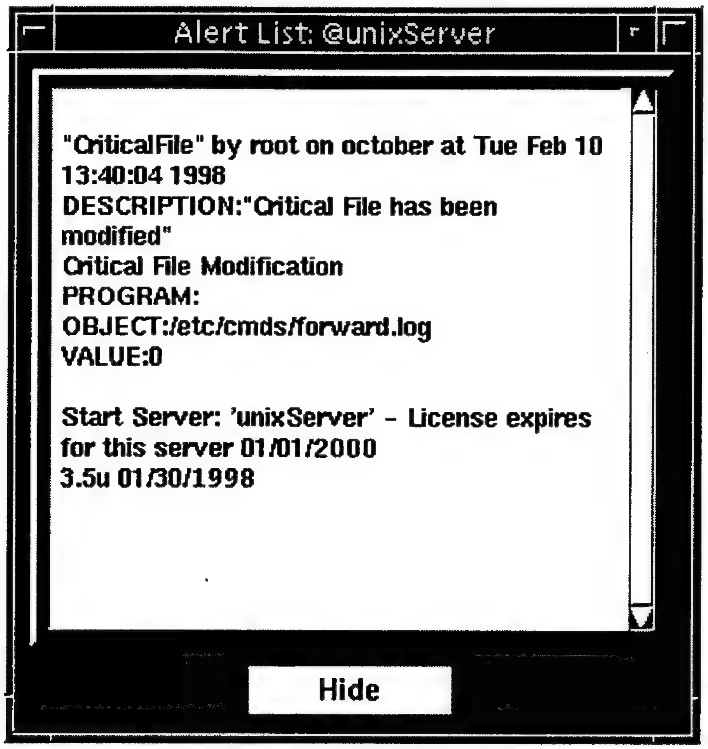


Figure 5.13. The Behavior Bar Graph Window. From Ref. [13].

D. ALERTS AND WARNINGS

CMDS generates alerts and warnings when a network user's behavior matches a predefined threat signature. Each target displays alerts in an Alert List window, shown in Figure 5.14. This window will appear on the screen when you start a CMDS target. If you are in real-time mode, alerts are displayed in real-time. If you are in batch or on-demand mode, alerts will display when processed. The most recent alerts appear in the foreground. The alert time, shown in the window, is the time of the event that caused the alert. If you select the Hide button to remove the Alert List window from your screen, the window will reappear as soon as the next alert occurs.

Note: In guiless mode, alerts and warnings are not displayed, but are saved in the CMDS database for future retrieval. [Ref. 13]



```
"CriticalFile" by root on october at Tue Feb 10
13:40:04 1998
DESCRIPTION:"Critical File has been
modified"
Critical File Modification
PROGRAM:
OBJECT:/etc/cmds/forward.log
VALUE:0

Start Server: 'unixServer' - License expires
for this server 01/01/2000
3.5u 01/30/1998
```

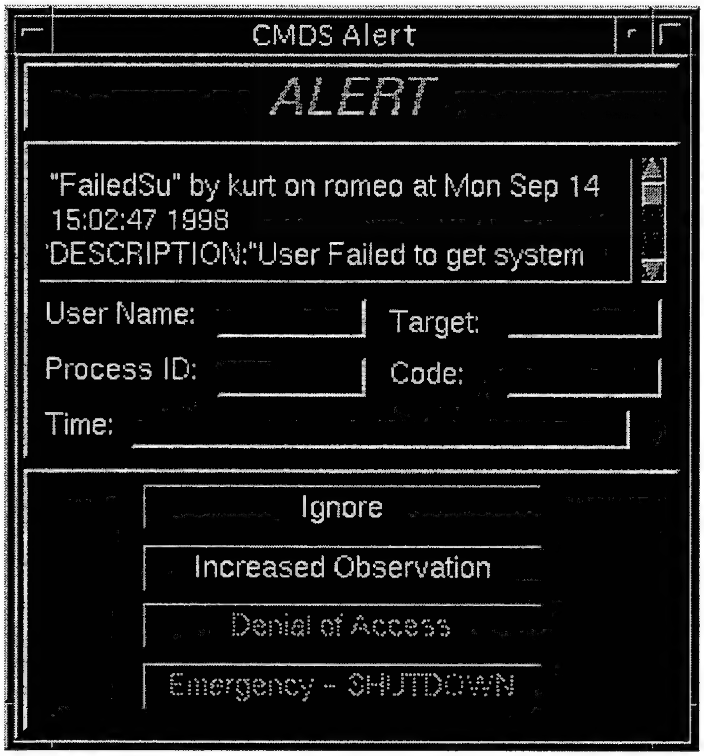
Figure 5.14. The Alert List Window. From Ref. [13].

When CMDS detects an alert, the red CMDS Alert window, shown in Figure 5.15, will pop up on your screen. The alert window will not automatically refresh, it remain on the screen until the user manually clears it. While the Alert List window allows you to view the sequence of alerts, the CMDS Alert window enables you to respond to a specific alert.

A scrollable box in the upper portion of the CMDS Alert window displays the alert message. The window contains the following fields: [Ref. 13]

- **User Name:** Name of the user who generated the alert
- **Target:** Name of the target machine
- **Process ID:** Process ID number

- **Code:** This field is for future use as a priority number for alerts
- **Time:** Date and time of the event that caused the alert



"FailedSu" by kurt on romeo at Mon Sep 14 15:02:47 1998
'DESCRIPTION:"User Failed to get system

Figure 5.15. CMDS Alert Window. From Ref. [13].

The current version of CMDS only provides two ways to respond to an alert. Simply select the action you want to take. [Ref. 13]

- **Ignore:** Closes the CMDS Alert window.
- **Increased Observation:** In real-time mode, this option allows you to view the CMDS Monitor window. This enables you to see the user's current activity, historical activity, a line graph, or a bar graph.
- **Denial of Access:** (Not implemented in V3.5.1.)

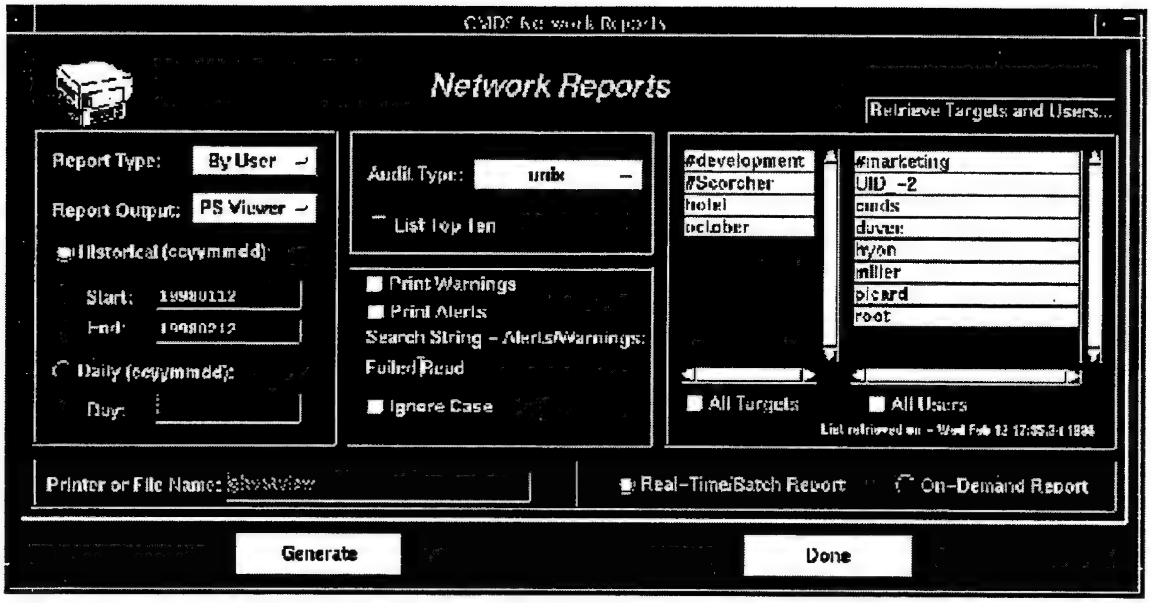
- **Emergency-SHUTDOWN:** (Not implemented in V3.5.1.)

A complete list of CMDS Alerts and Warnings for all systems is contained in Appendix A.

E. NETWORK REPORTS

CMDS also has the ability to present trending data in graphs and charts. Trending information is presented graphically to make it easier to identify patterns in the data. For example, the trending reports can identify when a user starts to work non-duty hours. If a user suddenly starts to work many non-duty hours, a graph will reveal this activity.

Network Reports display alphanumeric and bar graph information in an easy-to-read format. This allows you to design your network reports by selecting from a variety of options, including report type, report output, report range, audit type, top ten list, alerts and warnings, and single, or multiple targets and users. [Ref.13] To gain access the Network Reports window, go to the CMDS Control Window and select Network Reports. The Network Reports window will appear on the screen as shown in Figure 5.16.



Report Type: By User
Report Output: PS Viewer
● Historical (ccyymmdd):
Start: 19980112
End: 19980212
○ Daily (ccyymmdd):
Day:

Audit Type: unix
List Top Ten

■ Print Warnings
■ Print Alerts
Search String - Alerts/Warnings: Failed Read
■ Ignore Case

#development
#Scorcher
hotel
october

#marketing
UID -2
cmds
dover
hyon
miller
picard
root

■ All Targets
■ All Users
List retrieved on - Wed Feb 12 17:35:34 1998

Printer or File Name: ghostview
● Real-Time/Batch Report
○ On-Demand Report

Figure 15.6. The CMDS Network Reports Window. From Ref. [13].

Reports can display audit data by user, by target, by date, or by hour. You can use a search string to filter alerts and warnings. CMDS searches for the string you enter and produces a report with all occurrences of alerts and warnings containing that string. For example, the Security Administrator can use this capability to obtain a report of critical files accessed or a report of users who changed their privilege level. The report header identifies the search string.

The Network Reports window contains three sections. On the left side are the following fields and buttons: [Ref. 13]

- **Report Type:** Determines whether the X axis of a bar chart in a network report displays by user, by targets, by date, or by hour. The default display is By User. Select Report Type to access a drop-down menu with the available options. If you have selected the Daily Report option, the By Date option will not be available. The Report Type field also forms the basis for calculating averages and sorting alerts and warnings.

- **Report Output:** Provides a drop-down menu with options to print a hard copy of your report, view it on the screen with PS Viewer, or send it to a file. The Report Output default is the PS Viewer (GhostView) option.
- **Historical (CCYYMMDD):** Specifies a period of time greater than one day. This option requires you to enter data in the following fields:
- **Start:** The date for the first day of the report period in CCYYMMDD format.
- **End:** The date for the last day of the report period in CCYYMMDD format.
- **Daily (CCYYMMDD):** Used to choose a specific day for a report.
- **Day:** The day in CCYYMMDD format.

The middle section of the **CMDS Network Reports** window displays the following fields and buttons: [Ref. 13]

- **Audit Type:** Provides a drop-down menu that contains the target audit data used to generate a report. To receive a summary list of alerts and warnings generated by all applicable targets select All.
- **List Top Ten:** Generates a list of the ten users, targets, or dates that recorded the greatest number of alerts and warnings during the report period. This list will show the top ten users, targets, or dates, depending on your selection in the Report Type field.
- **Print Warnings:** Generates a list of warnings.
- **Print Alerts:** Generates a list of alerts.

- **Search String - Alerts/Warnings:** Enter a unique string of letters in this field to select alerts and warnings of a certain type. For example, to generate a report with an alerts and warnings list that includes only messages about critical files, enter Critical. Select the Ignore Case option to make the search string ignore upper and lower case designations.
- **Ignore Case:** Select the Ignore Case box to turn off case sensitivity. CMDS will then search for the characters you enter, regardless of upper or lower case.

The right section of the **CMDS Network Report** window lists the following information: [Ref. 13]

- **Retrieve Targets and Users:** Refreshes the lists of targets and users. The following messages appear when selected:

  Retrieving Target and User data from the database. This may take a few minutes, depending on size of data stored.
- **Targets:** Lists the targets of all the servers that CMDS has monitored data. Select the target or targets from this list that contain audit data you want to generate in a network report.
- **Users:** Lists all the users on all targets that CMDS has monitored data. Select the user or users from this list that contain audit data you want to generate in the network report.
- **List retrieved on:** Indicates by day of the week, month, date, hour, minute, and seconds the last time CMDS updated the user and target lists.

The bottom of the **CMDS Network Reports** window displays the following fields and buttons: [Ref. 13]

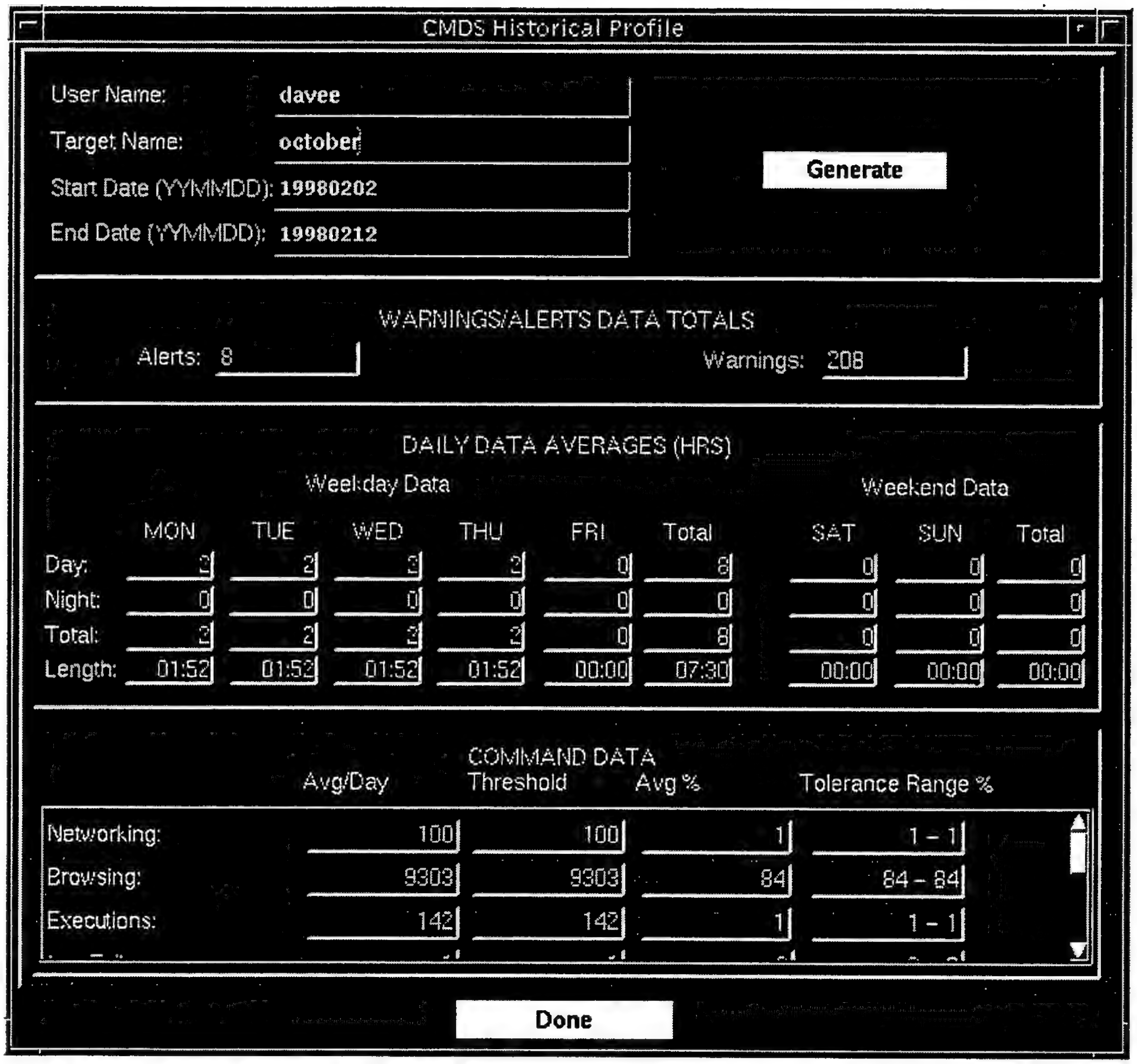
- **Printer or File Name:** Enter a filename or printer name, depending on your selection in the Report Output field.
- **Real-Time/Batch Report:** Select this option if you want the report to contain target audit data processed in real-time or batch mode.
- **On-Demand Report:** Select this option if you want the report to contain target audit data processed in on-demand mode.
- **Generate:** Select the Generate button to check on valid inputs and generate the report. If you have entered valid data, the following message appears: ***"Started Subprocess for Network Reports"***

F. CMDS PROFILES

CMDS offers the unique ability to generate specific profiles for specific users. These profiles can be custom generated and are based on the user's name, target host name, and dates. This feature allows the security administrator to perform either a historical profile and/or a daily profile on a user's behavior.

1. Historical Profiles

To generate a historical profile of a user's behavior, select the Historical Profile button on the Control Window. The Historical Profile window will appear as shown in Figure 5.17.



CMDS Historical Profile

User Name:	davee
Target Name:	october
Start Date (YYMMDD):	19980202
End Date (YYMMDD):	19980212

WARNINGS/ALERTS DATA TOTALS

Alerts: 8 Warnings: 208

DAILY DATA AVERAGES (HRS)

	Weekday Data						Weekend Data		
	MON	TUE	WED	THU	FRI	Total	SAT	SUN	Total
Day:	2	2	2	2	0	8	0	0	0
Night:	0	0	0	0	0	0	0	0	0
Total:	2	2	2	2	0	8	0	0	0
Length:	01:52	01:52	01:52	01:52	00:00	07:30	00:00	00:00	00:00

COMMAND DATA

	Avg/Day	Threshold	Avg %	Tolerance Range %
Networking:	100	100	1	1 - 1
Browsing:	9303	9303	84	84 - 84
Executions:	142	142	1	1 - 1

Figure 5.17. The CMDS Historical Profile Window. From Ref. [13].

The period of time between the start and end dates defines the historical data period. This period can include data as old as the date of the first audit record and as current as today's date. However, note that if the servers are running, the statistical data for the current day may not have been written to disk yet. Therefore, the report may not be current.

The Historical Profile window contains the following fields and buttons:

- **User Name:** The user you want to generate the historical profile.
- **Target Name:** The target host from where you want to extract the historical profile data.
- **Start Date (CCYYMMDD):** Start date of the historical data period.
- **End Date (CCYYMMDD):** End date of the historical data period.
- **Generate:** Generates the historical profile.

The WARNINGS/ALERTS DATA TOTALS section contains the following fields: [Ref.13]

- **Alerts:** Displays the number of alerts generated during the historical data period.
- **Warnings:** Displays the number of warnings generated during the historical data period.

The DAILY DATA AVERAGES (HRS) section displays the following fields categorized under Weekday Data (Monday through Friday) and Weekend Data (Saturday and Sunday): [Ref. 13]

- **Day:** Shows the average number of hours of a user's activity for each day of the week during the historical data period. The CMDS day is from 8:00 a.m. to 4:59 p.m.
- **Night:** Shows the average number of hours of a user's activity for each night of the week during the historical data period. The CMDS night includes the times from midnight through 7:59 a.m. and from 5:00 p.m. through 11:59 p.m.
- **Total:** Lists the total hours, day and night, for each day of the week during the historical period.

- **Length:** Displays the average length of the user's sessions for each day of the week during the historical data period.

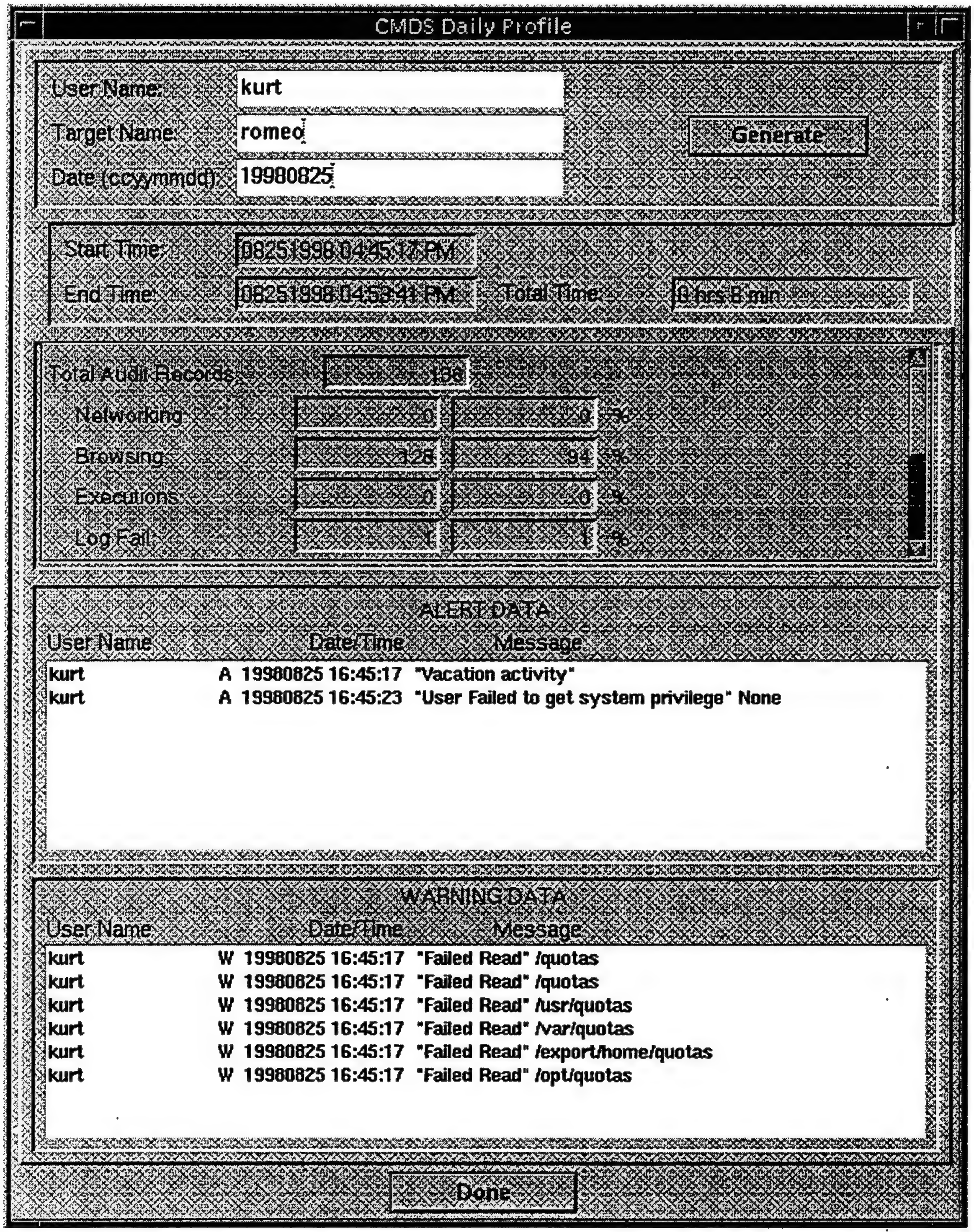
The COMMAND DATA section contains the following fields presented in table format for each statistical category: [Ref.13]

- **Avg/Day:** Displays the average number of audit records generated for each day the user is logged in during the historical data period.
- **Threshold:** Displays the threshold, which is the average per day plus the standard deviation of the historical data period.
- **Avg%:** Displays the average percentage of a record during the historical data period.
- **Tolerance Range%:** Displays the percentage range, which is the average percentage of plus and minus the standard deviation percentage of a record for the historical data period.
- **Done:** Closes the Historical Profile window.

If you enter invalid data, CMDS will notify you with an error message. Error messages and causes are listed in Appendix B.

2. Daily Profiles

CMDS provides a system administrator with the ability to generate a profile based on a user's behavior on a particular day. The Daily Profile window will appear (Figure 5.18) when selecting the Daily Profile button on the Control Window. The period of time between the start and end dates defines the data period. It can include data as old as the date of the first audit record and as current as today's date. If the servers are running, the statistical data for the current day may not have been written to disk yet and the report may not be accurate.



User Name: kurt

Target Name: romeo

Date (ccyymmdd): 19980825

Start Time: 08251998 04:45:17 PM

End Time: 08251998 04:53:41 PM Total Time: 0 hrs 8 min

Total Audit Records: 136

Networking	0	0	%
Browsing	128	94	%
Executions	0	0	%
Log Fail	1	1	%

ALERT DATA

```
User Name           Date/Time          Message
kurt            A  19980825 16:45:17  "Vacation activity"
kurt            A  19980825 16:45:23  "User Failed to get system privilege" None
```

WARNING DATA

```
User Name           Date/Time          Message
kurt            W  19980825 16:45:17  "Failed Read" /quotas
kurt            W  19980825 16:45:17  "Failed Read" /quotas
kurt            W  19980825 16:45:17  "Failed Read" /usr/quotas
kurt            W  19980825 16:45:17  "Failed Read" /var/quotas
kurt            W  19980825 16:45:17  "Failed Read" /export/home/quotas
kurt            W  19980825 16:45:17  "Failed Read" /opt/quotas
```

Figure 5.18. The Daily Profile Window. From Ref. [13].

The Daily Profile window contains the following fields and buttons: [Ref. 13]

- **User Name:** The daily profile of the user you want to generate.
- **Target Name:** The target host from where you want to extract daily profile data.
- **Date(CCYYMMDD):** The date for the daily profile you want to generate.
- **Generate:** Select the Generate button to create the profile.

CMDS displays daily profile data in the following fields: [Ref. 13]

- **Start Time:** Displays the time the user generated the first audit record on the given date.
- **End Time:** Displays the last time the user generated an audit record on the given date.
- **Total Time:** Shows the amount of time in hours and minutes between Start Time and End Time.
- **Total Audit Records:** Lists the number of audit records the user has generated since midnight.
- **Category Audit Records:** Displays audit records generated by category and the percentage of these records versus the total number of records.
- **Alert Data:** Lists all alert data generated by user name, date/time, and message.
- **Warning Data:** Lists all warning data generated by user name, date/time, and message.
- **Done:** Closes the Daily Profile window.

If you enter invalid data, CMDS will notify you with an error message.

G. TAILORING CMDS

For maximum flexibility, the CMDS Server uses an expert system to detect attack signatures. It can configure the system to define new alerts and warnings. C Language Production System (CLIPS) is an expert system tool, which provides a complete environment for the construction of rule and/or object-based expert systems.

Defining new alerts and warnings with CLIPS is a three-step process. [Ref. 13]

- Understand the attack signature of the new behavior that will generate the alert or warning.
- Define the facts, or data, that will be extracted from the incoming audit data and make the facts available to the expert system through the ***eventfacts*** file.
- Write the rules that recognize the attack signature pattern in the incoming data in the ***constructs.clp*** file.

1. Attack Signatures

Attack signatures are patterns found in audit records that indicate potential misuse. A good example of this concept is a Trojan horse, which is a destructive program that masquerades as a benign application. Unlike a virus, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer. Detecting Trojan horses is critical to maintaining a secure network of computers. Because there is no clear definition of a Trojan horse, the

CMDS server does not detect Trojan horses directly. Instead, it detects attack signatures that indicate Trojan horse activity.

One indication of Trojan horse activity is a privilege upgrade because processes seeking to do harm typically need to have expanded privileges to get to critical system files. This behavior is unique to Trojan horses because most processes needed by everyday users do not require expanded privilege. Privilege upgrade is therefore a good candidate for an attack signature.

2. Defining Facts

Facts are discrete pieces of information made available to the expert system that are processed for patterns of misuse behavior. An attack signature may be present in a single fact or a set of facts. The facts are maintained in the CMDS fact base, which is built by "asserting" facts through the eventfacts file. You can configure the server to assert facts based on specific CMDS record types. Each record processed that matches a number in the eventfacts file will be asserted as a fact in the CMDS attack signature fact base.

3. Writing Rules

The CMDS CLIPS Rule Base manipulates these facts, which you can configure based on your system-specific needs. Rule-based programming is one of the most commonly used techniques for developing expert systems. A rule contains an *if* portion and a *then* portion. The *if* portion is a series of patterns specifying the facts or data which cause the rule to be applicable. The *then* portion of a rule is a specific set of actions that are executed when the rule is applicable. Rules define the patterns of attack signatures and the text displayed in the alert boxes and summary reports.

H. SUMMARY

The Computer Misuse Detection System (CMDS) is designed to provide organizations with a monitoring capability that can be used to enforce a computer security policy. The power of CMDS comes from its ability to process large amounts of raw audit log information from many different sources, including Windows NT, UNIX , SUN/SOLARIS, TRUSTED SOLARIS, and RAPTOR. The compiled information is then presented in a user-friendly format. CMDS can be configured to process data in three different modes, Real-Time, Batch, or On-Demand, and allows an organization to set-up CMDS based on their individual requirements.

The processed data can be displayed in various forms, depending on the needs of the administrator. For example, a user's current activities can be monitored or a historical account of his or her activities can be displayed. Some other features of CMDS include, the ability to generate network reports, historical profiles, and daily profiles. Additionally, predefined warnings and alerts will pop up on the administrator's screen indicating potential wrong-doing. Another significant advantage of CMDS, is its ability to be modified to fit into any organization's computer security policy. CLIPS is an expert system tool that can be used to define new alerts and warnings and tailor CMDS.

VI. POLICY

A. INTRODUCTION

Computer systems are an essential part of all organizations. In order to ensure that these computer systems are used in a proper and effective manor, it is critical that a formal set of acceptable standards be established. System administrators and users should be aware of these standards and regularly trained on computer security issues. A set of acceptable standards for computer system use can best be implemented through a well-defined computer security policy.

A computer security policy is a formal document that defines rules and principles that affect the way an organization approaches computer security related problems. Additionally, it establishes agreed upon conditions for the use of the organizations computer resources. The goal of a computer security policy is to prevent the loss of information that is critical to an organization. Failure to follow these guidelines could easily lead to such a loss, regardless of whether the security breach occurred as a result of an act of god, hardware/software error, or malicious action, internal or external, to the organization.

Computer security requirements can greatly vary from organization to organization. It is important that each organization reviews its security requirements and formulates its own computer security policy.

B. PURPOSE OF A WRITTEN POLICY

There are many reasons to have a formal written policy. The most obvious of which is "because we have to." [Ref. 14] Many organizations are bound by a set of common practices that are reviewed or audited periodically for compliance. Government organizations are no different, and in many cases require a more strict set of rules to enforce national security issues. Written policies and procedures help assure that employees consistently and properly carry out the work needed to manage an organization.

Another significant reason for the development of a written policy is to help guide the behavior of employees who are constantly faced with numerous decisions. This applies to occupations such as physicians, accountants, lawyers, scientists and other professionals that require a set of well-defined procedures in order to accomplish their job. Once policy is in place, personnel that have been trained on the set of rules can be, in theory, interchanged. With the constant turn over of personnel, the military relies on these procedures to accomplish its mission. Every process, from how to operate a engineering plant on a warship to pre-flight check list for pilots has a written set of formal procedures that must be performed the same way every time to ensure the completion of the mission and the safety of personnel.

Policies also allow for the smooth turnover of personnel. The military constantly transfers people every few years. It is extremely important that the person taking over a job can adequately and properly perform the assigned duties. Written policies are invaluable tools that ensure the consistently and accuracy of the work being accomplished.

Policies must be flexible enough to allow for the ever-changing environment. They must to incorporate a way of handling unique situations that might arise. Policies that have a special way of dealing for changes can form a directory of operating procedures used in irregular and unique situations. Additionally, they can describe various special situations and provide a thought process for handling these situations. While handling these unique situations is very important, it is also important to allow for a feedback mechanism. A feedback mechanism would allow the policies and procedures to be updated and thus the best procedures would be followed.

Finally, written policies form a critical component of the management philosophy. They reflect intangible operations, management theories, and technical directives that are produced in boardroom meetings. The written procedure contained in the policy ties the abstract thought process to a solid work task. [Ref. 14] A directive must be converted into a formal written policy statement that is clearly written, specific, and unambiguous. The policy statement of any organization, especially as it relates to computer security practices, is where the executive mentality is manifested into the daily organization operations. [Ref 14]

C. TYPES OF POLICIES

The world is full of many organizations with many different needs when it comes to computer security. While policies should be tailored to an organization specific need, some general classifications of computer security policies have been developed. The three general classifications are regulatory, advisory, and informative. It is important to understand that while these three types of policies exist; no organization can properly function using just a single type of policy. Combinations of policies are often necessary to handle the different levels of sensitive information that are contained within any organization.

1. Regulatory

This type of policy is primarily for organizations that are not totally at liberty to develop and carry out security policies. They are usually organizations that are frequently held to close public scrutiny and operate in the public interest or public safety. However, they could be organizations that are responsible for managing large amounts of money for constituents such as brokerages, banks, or insurance companies. These policies describe in great detail what is to be done, when it is to be done, and who is to do it. [Ref. 14] It contains specific references to job function, transactions, and procedures that are unique to a specific organization.

They are two reasons for establishing this type of computer security policy. The first reason is to establish a clearly consistent process. This is very important for organizations that are involved with the general public. Policies Must show uniformity in the way regulations are carried out without prejudice. The second reason is to allow individuals that are unfamiliar with the process to have confidence in those who are doing the job.

While this type of policy touches on procedures in great detail, it does have a down side. It is not very effective in situations where personnel are making judgements based on the current facts and environment. An example would be the decision to send an ambulance to a victim of an attack. The rescue squad, attempting to save a life, does not have the time to follow an extensive process. Additionally, this policy would not be practical when the situation requires frequent variations from the prescribed method. A regulatory policy that has too many exceptions is cumbersome, difficult to enforce, and can lead to non-compliance of personnel who take exception to every rule.

2. Advisory

The primary objective of this type of policy is to give trained personnel the opportunity to quickly and easily identify a standard course of action, while allowing them the freedom to make judgement decisions when special situations arise. While an advisory policy is not as rigorously enforced as a regulatory policy, the risk of not following the policy is usually stated in the policy. This statement is an attempt to allow personnel referencing the policy to make an informed decision based on the facts surrounding the situation. When developing this type of policy it is important to consider the risk involved. Some risk might include: [Ref. 14]

- Omitting information needed to make a valid decision.
- Failing to notify the appropriate decision-makers need to complete the process.
- Missing important deadline or due dates.
- Lost time reviewing nonstandard processes.

This policy is only advisory in nature and an organization that is considering using this type of policy must consider the risks and the experience level of its personnel. It is conceivable that one organization might apply this policy to its most experience personnel, while another might use it as a required policy. It could also apply to specific types of procedures. For example, a policy may require two authorizing signatures to obtain a password for changing a production computer program. It may be advisory under normal circumstances, but could be disregarded or replaced with an alternative policy in the event of an absence of a key individual. This type of situation must be described and identified within the policy so all personnel are aware of the deviation in policy.

3. Informative

An informative policy is the least directive in nature and is one that simply informs the user. No actions are expected and no penalty of risk is imposed for not following the policy. The overall goal of an informative policy is to inform as many people as possible. While this type of policy is much less restrictive than a regulatory or advisory policy, it often carries strong messages and delineates extremely severe consequences. For example, it can state "future use of this system or process is restricted to authorized individuals and violators will be prosecuted." This statement is informative in nature. While authorized users will have no negative consequences to their actions, it implies that unauthorized users that insist on ignoring the warning of the policy will have severe consequences.

A major advantage of having an informative policy is that an organization can have the policy widely distributed among its employees without the risk of sensitive information being disclosed. The policy can refer personnel, who deal with sensitive information, to an alternate policy that contains the detailed procedures needed to complete the task and is not widely distributed. An example could read: "Passwords will be changed in accordance with department standards. See your department password policy for further information." [Ref. 14] This type of statement would inform personnel that a password policy exists, but only gives that information to authorized personnel who have access to the policy. When using an informative policy in this way, it is important to ensure that all associated references are kept up to date and well organized.

D. COMPONENTS OF POLICIES

While there are many different types of policies covering numerous different procedures and guidelines, they all contain the same common components. Depending on the policy, these components may be defined explicitly or they could be less defined and require careful reading of the policy to extract them. Regardless of whether the policy is explicit or implicit in its description of the commponents, nearly all effective policies contain the ten items described in this section. [Ref. 14]

- **Statement of Policy:** This is the most important part of any policy. It is a brief, clearly written statement that states in words what is to be expected of personnel. It must give the reader enough information for them to decide whether provisions of the policy bind them. Additionally, it must imply whether it is a policy oriented towards people, procedures, equipment, money, or communications, etc.
- **Authorizing Executive/Officer:** Most often this is the senior executive officer of the organization. This is the person who has the overall responsibility to ensure the organization's adherence to the policy.
- **Policy Author/Sponsor:** This is the name of the individual or group of individuals that developed the policy. The name(s) should be contained within the policy itself, therefor allowing any questions, comments, interpretations, or clarifications to be addressed directly to the authors.

- **Reference to Other Policies and Regulations:** In many cases policies are related to other policies or procedures that already exists. Because changes in these referring policies may affect related policies, this reference makes maintenance of the policy structure easier to administer and more responsive to normal changes.
- **Measurement Expectations:** Conforming to policies is not always followed by a simple yes or no answer. Conditions that need to be clarified in a security policy, but would make the wording overly complicated and long-winded can be included in this section.
- **Process for Requesting Exception:** This is a statement of the process for which exceptions can be requested. If they are no exceptions it should be so stated. This should not be a section that defines the conditions under which exceptions will be granted or a list of possible exceptions, but only the process to requesting an exception. Being too explicit in defining the acceptable exclusions will lead to receiving an abundance of exception request.
- **Process for Requesting Change of Policy:** All successful policies have a built-in procedure to allow for change. In some cases the change may only be a technical review, in others a full overhaul of existing procedures may be needed to account for shifts in technology, management styles, or organizational philosophies.
- **Action Upon Violation:** A policy with no punishment when violated should not be a policy. At a minimum, this section should include an acknowledgement by the violator's supervisor that the policy has been

correctly followed. Depending on the sensitivity of the policy, a violation could result in job termination or, in some cases, legal action being taken. In these situation it is important that the policy make a statement to the effect of "....violation may result in termination of employment and/or legal action." [Ref. 14]

- **Effective Date:** All policies need to given a date for which they are to be effective. This date should not be prior to the release date of the policy, however prior events can be included as a Measurement Expectation or actually stated in the policy statement.
- **Sunset or Review Date:** Every policy should have an expiration date or a reconfirmation date. This is important because this date will ensure that the policy is reviewed periodically.

E. POLICY CONSIDERATIONS

1. Risk Assessment

Conducting a risk assessment is an important step in developing a security policy. There are 3 basic questions to ask when performing a risk assessment. These are: 1) What am I trying to protect? 2) What do I need to protect against? 3) How much time, effort, and money am I willing to expend to obtain adequate protection? [Ref. 15] It is very important to know the value of the information you are trying to protect, what the threat to the information could be, and how much money you are ready to pay to protect it. To do this, there are three steps that should be taken. These are: 1) Identify the assets to be protected, 2) identify the threat to each asset, and 3) calculate risks. In identifying assets, accounting of tangible assets such as computers, proprietary data, technical manuals and books, printouts, personnel and audit records should be considered. Also, intangibles such as safety of personnel, privacy of users, passwords, and company reputation should be considered. Threats to consider would certainly include environmental threats like earthquake, flood, or fire. Other threat considerations could be illness or loss of key personnel, loss of network services, loss of utilities, viruses, data theft, or malicious insiders. Once the risks are identified, they must be quantified as to their importance. Risk calculation involves the cost incurred due to loss of an asset. Time is money therefore the amount of time assets are off-line due to failure must be considered as well as total losses. Risk considerations would include non-availability for specified periods of time, loss or destruction, and unauthorized disclosure within the organization or to outsiders. Security comes with a price. Based on the assets to protect, threat to these assets, and the cost of losing these assets, through cost-benefit analysis, a determination can be made as to the value of information and how much money should be spent on its protection.

2. Trade-offs

Tight security can be expensive and usually involves inconvenience to the users. As each layer of security is added to a system, the user must authenticate access through these layers to carry out tasks. How much inconvenience the users are willing to accept should not be a consideration. But the amount of time consumed by users due to tight security is a consideration. A balance must be found. Once again, the risk to assets and cost of loss is the primary focus.

Manpower placed on the security team should be of primary importance. Computer security should never be a collateral duty unless the information and assets protected are of negligible value. Therefore, money spent on a well-trained security team should be proportional to the value of the assets protected.

3. Training

Initial training should be conducted with each new employee. This training must contain training designed to promote security policy, enhance user knowledge of the system, and emphasize the consequences of poor security. Also included in this training would be the penalties for failure to observe policy.

Periodic training should be conducted to keep users abreast of current threats as well as providing refresher training on old topics. The frequency of this training would be based, once again, on how well the systems assets should be protected. Time in training, although not time that users are being productive, will be time well spent in the long run.

Training reviews should be conducted on a periodic basis. These reviews are for the purpose of assessing how well users are being trained. Review methods would include a review of security failures, personnel questionnaires and security quizzes, or other logged incidents that could affect security.

F. POLICY GUIDELINES WHEN MONITORING

1. Monitor Capabilities

When writing a security policy, and a plan is in place to conduct internal system monitoring, the monitoring must be incorporated into the policy and the training plan.

Once the monitor's capabilities are understood, these capabilities can become the core considerations within a security plan. These monitoring capabilities, once taught to the users, will provide them with an awareness of security wrong-doing and make them aware of the fact that they are being monitored on the job. Placed in the context of "monitoring to enforce policy" and not "monitoring to catch people goofing off," it will be easier to sell the idea to the users. The importance of protecting system assets must always be emphasized, in policy and training.

2. Monitor Implementation

The implementation of the monitor requires careful consideration. How often is monitoring desired? How much overhead is acceptable? What features will be enabled/disabled? A thorough review of the monitor documentation prior to installation is of utmost importance. The frequency of monitoring can also determine the size of the security team. For example, if monitoring is required for a system that is used 24 hours per day, then real-time monitoring might be desired. For real-time monitoring, it would be desirable to have a security response team to respond to alerts from the monitor. If the protected assets are considered "not worth" constant monitoring due to the overhead involved or for other reasons, batch processing on a set schedule might be the best choice. Then again, perhaps monitoring on a random basis is desired. Once all possible options are considered, and the choice of monitoring frequency is made, then installation can begin. Now the features you wish to activate must be known. During setup, the configuration must be documented and set forth, step by step, in the security policy as a guideline in the event the system fails and the monitor must be reinstalled. Changes to the monitor configuration should be carefully recorded and maintained. Not only will this record an accurate configuration, but it will provide a record of previous configuration in the event something goes wrong during a configuration change.

3. The Monitoring Team

A team of well-trained and qualified security professionals should make up the monitoring team. The computer security manager would oversee this operation or be the team leader. It would probably be best to have one person, well-trained in monitoring, to head the team under the oversight of the security manager. Once again, the question of "How much risk is acceptable?" must be asked. Along with the frequency of monitoring, the makeup of the monitoring team is dependent on this frequency. Naturally, a real-time monitoring operation can require a 24 hour response team although not necessarily. The system may continue to monitor real-time in the background while not sending out alerts until the security team reports for normal daytime duty. But if the information protected is so vital, and perhaps questionable employees are involved, a 24 hour manned response team might be the best choice.

G. SUMMARY

A well-written and effectively communicated computer security policy can greatly help an organization prepare for the twenty-first century. By specifying the goals of an organization, at it relates to computing, the computer security policy can improve the efficiency of an organization, provide employees with a clear direction, and protect sensitive information. While policies should always be tailored to an organization's specific needs, they generally fall into three categories: regulatory, advisory, and informative. When developing a security policy it is important to consider risk assessment, trade-off, and employee training. Additionally, if a monitoring capability is available, or desired, it must be incorporated into the security policy and training plan. Once the employees have been fully trained, the monitoring capabilities could become the foundation of an organization's computer security policy.

VII. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSION

This thesis addresses internal threats to system security, profiling and monitoring, and considerations for establishing a policy to incorporate profiling and monitoring as an integral part of an overall security plan. Time and again, statistics are issued by various organizations that state at least seventy percent of all security breaches are caused by insiders—intentional or accidental. [Ref. 1] One way to mitigate the risk of security breaches is to enforce security policy by monitoring computer systems. With classified information on many military computer systems, we believe it would be highly worthwhile to monitor these systems for suspicious activity. Computer profiling software is available today and can perform many of the functions needed to protect sensitive information by monitoring user activity on the computer system.

B. RECOMMENDATIONS

With the complex and diverse computer systems available today, a monitoring system must be capable of handling this diversity. For example, a network that incorporates both Unix and Windows NT operating systems would need a monitor capable of "seeing" both systems. This mix of operating systems currently exists in the Navy today. Any monitoring application chosen for security duty must be capable of monitoring a distributed system. CMDS has the capability of monitoring both Unix and Windows NT.

C. TOPICS FOR FURTHER STUDY

C Language Integrated Production System (CLIPS) is an expert system tool that may be used to refine and tailor the Computer Misuse Detection System (CMDS). Although our research did not allow us to look into the usefulness of this tool, it is available and worth the research to determine if it would enhance the monitoring capabilities needed for the monitoring and protection of classified military information systems.

It was difficult to experiment with CMDS due to the need to have root passwords to adequately set up and continually monitor the package. It would be invaluable to run CMDS on a large network to achieve some real, tangible data on this application or an application of equivalent merits under the supervision of a system administrator. The limited size of the lab we used did not provide a sufficient testbed. A testbed needs to be constructed and made available for future experiments.

In addition to monitoring a large network, research into monitoring access to classified files is needed. Assignment of users to clearance levels and compartments, then monitoring to detect access to information above a user's clearance level and compartments could enhance the protection of classified information on military computer systems.

One possible research topic could be the use of Border Gateway Protocols (BGPs). A BGP is a protocol for exchanging routing information between gateway hosts in a network of autonomous systems and is often the protocol used between gateway hosts on the Internet. The primary function of a BGP system is to exchange network-reachable information, this includes information about the list of autonomous system paths with other BGP systems. With the increasing reliance on the Internet, research on how to incorporate BGP systems and CMDS into workable computer security policy is needed.

Firewalls are critical to the success of secured connections to external networks and the Internet. [Ref. 14] While this thesis discusses the internal threats to computer systems, it would be beneficial to look at how CMDS and firewalls would react and how to incorporate them both into a well-defined computer security.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. CMDS ALERTS AND WARNINGS [Ref. 13]

SUN/SOLARIS ALERTS AND WARNINGS

CMDS Alerts for Sun/Solaris

ALERT ID	SOLARIS EVENT #	ALERT MESSAGE	INTERPRETATION	FLAGS
4	18	***Accounting Changed***	CMDS generates this alert when a network user turns the accounting stream on or off.	ad
16	4, 6, 10, 42, 76, 77, 78, 79 ,80, 81, 82, 83	***Attempted critical file modification***	CMDS generates this alert when a network user attempts to modify a critical file or make changes to file content.	ad, fc, fd, fr, fw
9	6159	***Failed SU***	CMDS generates this alert when a network user attempts to gain the SU privilege and fails. Superuser is a privileged account on all systems and bypasses controls.	lo
13	10	***File Mode Setuid***	CMDS generates this alert when a network user sets a file's setuid bit. The setuid bit on a file allows a process to change the file's privilege level. The setuid bit is one way computer hackers and viruses can disrupt the system.	ad
11	40	***Privilege Upgrade***	CMDS generates this alert whenever a process changes a file's privilege. Setuid files must change process user ID during execution to change privilege level.	pc
7	--	***Sendmail Attack***	CMDS generates this alert when network users connect to a target machine via sendmail without a login. Older versions of operating systems allow a user to run an executable on the sendmail port.	--
2	23	***System Reboot*** ***System Shutdown***	CMDS generates these alerts when a network user reboots or shuts down a machine that may adversely affect resource availability.	pc, ex
14	6154 or 6155	***Tagged Users***	CMDS generates this alert when a network user you have tagged in the ***taggedusers*** file logs on to a target machine.	lo
8	6154 or 6155	***Three logfailures***	CMDS generates this alert whenever a network user has had three password failures.	lo
24, 25, 26, 27, 28, 29, 30, 31	--	***Threshold Alert***	The threshold is the historical average number of records in a daily profile for a category plus one standard deviation. CMDS generates an alert whenever a network user has exceeded the threshold in a statistical category. The number of profile days can be configured in the minimum profile field at **$CMDS_DIR/targets/<target type>/config/configuration.<target type>**.	--
32	--	***Vacation Activity***	CMDS generates this alert when a user who is on the ***vacation list*** starts generating audit data. The ***vacation list*** indicates periods of time that the named user should not be generating audit data.	--

CMDS Warnings for Sun/Solaris

WARNING ID	SOLARIS EVENT #	WARNING MESSAGE	INTERPRETATION	FLAGS
12	8	*CD Outside $HOME*	CMDS warns you when a network user changes his working directory to be outside of his home directory.	fc
15	72, 73, 74, 75, 80, 81, 82, 83	*Failed Read*	CMDS warns you whenever a failed read occurs for a file. Read failures can indicate many things, including file browsing, bad path parameters, and other system behaviors which affect performance.	fc, fd, fr, fw
10	6159	*Successful SU*	CMDS warns you when a network user gains the SU privilege. When a user attains system privileges, he can bypass all controls.	lo

TRUSTED SOLARIS ALERTS AND WARNINGS

CMDS Alerts for Trusted Solaris.

ALERT MESSAGE	INTERPRETATION
Accounting Change	CMDS generates this alert when a network user changes accounting status.
Adjtime used	CMDS generates this alert when adjtime is used to change a system's internal clock.
Administrative Threshold	CMDS generates this alert when the threshold for administrative use is exceeded.
Application Threshold	CMDS generates this alert when the threshold for an application is exceeded.
Browsing Threshold	CMDS generates this alert when the threshold for browsing is exceeded. File browsing is a serious problem in today's multi-user environments.
Core dump	CMDS generates this alert when a process has dumped core.
Critical File	CMDS generates this alert when a user modifies a critical file or makes changes to file content.
Dev Alloc Threshold	CMDS generates this alert when the threshold for device allocation is exceeded.
Device alloc	CMDS generates this alert when a user allocates the CD-ROM drive, the floppy drive, or the microphone. A user who allocates the floppy drive often may be writing data to a "single-level device," which does not understand security labels.
DisableAudit	CMDS generates this alert when a network user disables auditing.
Eeprom changed	CMDS generates this alert when a network user changes eeprom (electrically erasable programmable read-only memory).
Executions Threshold	CMDS generates this alert when the threshold for executions is exceeded.
Host name set	CMDS generates this alert when a network user sets up a host name.
Log Fail Threshold	CMDS generates this alert when the threshold for log failures is exceeded.
MailAttack	CMDS generates this alert when a network user connects to a target machine via sendmail without a login. Older versions of operating systems allow a user to run an executable on the sendmail port.
Networking Threshold	CMDS generates this alert when the threshold for networking is exceeded.
PasswordFail	CMDS generates this alert whenever a network user has three password failures.
PrivilegeUpgrade	CMDS generates this alert whenever a process changes a file's privilege. *Setuid* files must change process user ID during execution to change privilege level.
Process Operations Threshold	CMDS generates this alert when the threshold for process operations is exceeded.
Read Fail Threshold	CMDS generates this alert when the threshold for read failures is exceeded. Read failures can indicate file browsing, bad path parameters, or other system behaviors which may affect system performance.
Reboot	CMDS generates this alert when a network user reboots a target system.
X Security Events Threshold	CMDS generates this alert when the threshold for X security events is exceeded.
Set Security Attr Threshold	CMDS generates this alert when the threshold for setting security attributes is exceeded.
Settimeofday used	CMDS generates this alert when a network user re-sets the time of day.
SetuidRoot	CMDS generates this alert when a network user sets a file's setuid bit. The setuid bit on a file allows a process to change the file's privilege level. The setuid bit is one way computer hackers and viruses can disrupt the system.

Shutdown	CMDS generates this alert when a network user shuts down a target system.
Superuser Threshold	CMDS generates this alert when the threshold for superuser activity is exceeded.
TaggedUser	CMDS generates this alert when a tagged user logs on to a target machine.
Total Records Threshold	CMDS generates this alert whenever a user has exceeded a threshold. A threshold is the historical average number of records in a daily profile for a category, plus one standard deviation. The number of profile days can be configured in the Minimum Profile field at $CMDS_DIR/targets/<target type>/config/ configuration.<target type>.
Trusted Fac Mgmt Threshold	CMDS generates this alert when a user manipulates the "Trusted Path" to change some part of they system.
Unattrib. Events Threshold	CMDS generates this alert when the threshold for unattributable events is exceeded.
Vacation Activity	CMDS generates this alert when a user who is on the *vacation list* starts generating audit data. The *vacation list* indicates periods of time that the named user should not be generating data.

CMDS Warnings for Trusted Solaris.

WARNING MESSAGE	INTERPRETATION
Added role	CMDS generates this warning when a network user adds a role.
Added user account	CMDS generates this warning when a network user adds a user account.
Change label failed	CMDS warns you when a network user attempts to change a label but fails.
Change label succeeded	CMDS warns you when a network user successfully changes a label.
ChangeDirectory	CMDS warns you when a user changes his working directory to be outside of his $Home directory. This could indicate file browsing which is a serious problem in today's multi-user environments.
Chown used	CMDS warns you when a network users changes file ownership by chown.
Client not privileged	CMDS generates this warning when a network user tries to utilize an unauthorized privilege.
Covert channel used	CMDS generates this warning when a network user uses a covert channel.
Crontab create	CMDS generates this warning when a user creates a crontab entry.
DAC access denial	CMDS generates this warning when a user attempts to access a file on which discretionary access has been placed.
Enable login	CMDS generates this warning when the system first boots up, and a user with the proper authorization logs in to enable the system to be used by normal users. Multiple instances of this warning would indicate multiple reboots.
Exportfs used	CMDS generates this alert when a file system is exported with exportfs.
Failed Read	CMDS warns you whenever a failed read occurs for a file. Read failures may indicate many behaviors, including file browsing, bad path parameters, or other system behaviors which affect performance.
Fchown used	CMDS generates this alert when fchown is used to change the owner and group of a file.
File privilege failed	CMDS generates this warning when a user's set file privilege fails.
Ftpd access denial	CMDS generates this warning when a network user attempts to access an FTP daemon but fails.
Ftpd authentication	CMDS generates this warning when a network user attempts to authenticate an FTP daemon but fails.
Ftpd login	CMDS generates this warning when a network user attempts to login to an FTP daemon but fails.
MAC access denial	CMDS generates this warning when a user attempts to move data from a file or directory with Mandatory Access Control.
Modified role	CMDS generates this warning when a network user modifies a role.
Mount used	CMDS generates this warning when a network user uses mount to mount a device.
Newgrp	CMDS generates this warning when a network user creates a new group using the newgrp command.
Ptrace used	CMDS warns you when a network user uses ptrace.
Security attr changed	CMDS generates this warning when a user changes security attributes.
Sensitivity label downgrade failed	CMDS generates this warning when a user attempts to downgrade a sensitivity label but fails.
Sensitivity label upgrade failed	CMDS generates this warning when a user attempts to upgrade a sensitivity label but fails.
Set file privilege	CMDS warns you when a network user modifies a set file privilege.

Setcmwlabel	CMDS warns you when a network user changes setcmwlabel.
Setdomainname used	CMDS generates this warning when a network user uses setdomainname to create or change a domain name.
Setregid used	CMDS generates this warning when a network user uses setregid.
Setreuid used	CMDS generates this warning when a network user uses setregid.
SuccessfulSU	CMDS warns you when a network user gains superuser privilege. When a user attains system privileges, he can bypass all controls.
Tnetd turned off	CMDS generates this warning when a user turns off a telnet daemon.
Umount used	CMDS generates this warning when a user uses umount to unmount a device.
Vtrace used	CMDS warns you when a network user uses vtrace
Xtarget conn	CMDS warns you when a network user makes an X target connection.

WINDOWS NT ALERTS AND WARNINGS

CMDS Alerts for Windows NT.

Alert Message	Interpretation
Attempted critical file modification	CMDS generates this alert when a network user attempts to modify a critical file to gain access privileges.
Audit events discarded	CMDS generates this alert when the event log has reached the maximum size and has started to automatically delete the oldest events.
Audit log has been cleared	CMDS generates this alert when the event log has been cleared automatically or manually.
Audit policy has been changed	CMDS generates this alert when audit attributes have been modified.
Privilege Use Failed	CMDS generates this alert when an unsuccessful privilege change is attempted (i.e., administrator logoff).
Special Privilege Used	CMDS generates this alert when a role requiring special privileges (i.e., administrator logon) is used.
System Reboot *System Shutdown*	CMDS generates this alert when a network user shuts down machines and adversely affects resource availability.
Tagged Users	CMDS generates this alert when a tagged user logs on to a target machine.
Three logfailures	CMDS generates this alert whenever a network user has three password failures.
Vacation Activity	CMDS generates this alert when a user who is documented as being on the ***vacation list*** starts generating audit data. The ***vacation list*** indicates periods of time that the named user should not be generating audit data.

CMDS Warnings for Windows NT.

Warning Message	Interpretation
Administrative Function Used	CMDS warns you when a function requiring special administrator privilege is successful (i.e., new user added or deleted).
Failed Read	CMDS warns you whenever a failed read occurs for a file. Read failures may indicate many behaviors, including file browsing, bad path parameters, or other system behaviors which affect performance.
Special privilege used	CMDS warns you when a new login shows that a user has special privileges (i.e., administrator).
User logon	CMDS warns you when any user logs on to the NT target machine.

HP/UX ALERTS AND WARNINGS

CMDS Alerts for HP/UX.

Alert Message	Interpretation
Attempted critical file modification	CMDS generates this alert when a network user attempts to modify a critical file to gain access privileges.
Auditing disabled	CMDS generates this alert when a network user attempts to disable the CMDS audit stream.
Failed SU	CMDS generates this alert when a network user attempts to gain SU privilege and fails. Superuser is a privileged account on all systems and bypasses controls.
Privilege Upgrade	CMDS generates this alert whenever a process' user ID level is changed. Setuid

	files must change process user ID during execution to change privilege level.
System Reboot	CMDS generates this alert when a network user reboots a machine and adversely affects resource availability.
Tagged Users	CMDS generates this alert when a tagged user logs on to a target machine.
Threshold Alert	CMDS generates this alert whenever a network user has exceeded the threshold in a statistical category. A threshold is the historical average number of records in a daily profile for a category, plus one standard deviation. The number of profile days can be configured in the Minimum Profile field at **$CMDS_DIR/targets/<target type>/config/ configuration.<target type>.**
Vacation Activity	CMDS generates this alert when a user who is documented as being on the ***vacation list*** starts generating audit data. The ***vacation list*** indicates periods of time that the named user should not be generating audit data.

CMDS Warnings for HP/UX.

Warning Message	**Interpretation**
CD Outside $ HOME	CMDS warns you when a network user changes his working directory to be outside of his home directory.
Failed Read	CMDS warns you whenever a failed read occurs for a file. Read failures can indicate many things, including file browsing, bad path parameters, or other system behaviors which affect performance.
Successful SU	CMDS warns you when a network user has been successful and gained the SU privilege. Superuser is a privileged account on all systems and bypasses controls.

INTERLOCK ALERTS AND WARNINGS

CMDS Alerts for InterLock.

ALERT MESSAGE	DESCRIPTION	INTERPRETATION
RootLogin	Login as ROOT on the Firewall	User logged on to firewall as ROOT
ConsoleLogin	Login on Firewall Console	User logged on to the Administrator Console
FtpRoot	Ftp login as ROOT	User logged on to FTP as ROOT
InboundConnections	Repeated Inbound Connections	X (configurable) inbound attempts within Y (configurable) minutes

CMDS Warnings for InterLock.

WARNING MESSAGE	DESCRIPTION	INTERPRETATION
AolConnections	Threshold: AOL Connections	AOL connections exceeded historical profile threshold for private side address
AolInBytes	Threshold: AOL Bytes IN	AOL Bytes IN exceeded historical profile threshold for private side address
AolOutBytes	Threshold: AOL Bytes OUT	AOL Bytes OUT exceeded historical profile threshold for private side address
FtpConnections	Threshold: FTP Connections	FTP connections exceeded historical

		profile threshold for private side address
FtpFailLogin	FTP Failed Login	Failed FTP login on private side
FtpInBytes	Threshold: FTP Bytes IN	FTP Bytes IN exceeded historical profile threshold for private side address
FtpOutBytes	Threshold: FTP Bytes OUT	FTP Bytes OUT exceeded historical profile for private side address
FtpUnauthConn	FTP Unauthorized Connection	Failed FTP connection because of denial of permission
FtpUnauthDest	FTP Unauthorized Destination	Failed FTP connection because of invalid IP address
Http Connections	Threshold: HTTP Connections	AOL connections exceeded historical profile threshold for private side address
HttpInBytes	Threshold: HTTP Bytes IN	HTTP Bytes IN exceeded historical profile threshold for private side address
HttpOutBytes	Threshold: HTTP Bytes OUT	HTTP Bytes OUT exceeded historical profile threshold for private side address
HttpPasswdExpired	Password expired for http user	HTTP password has expired
HttpUserUnk	HttpUser Unknown	Failed HTTP connection because user is unknown
Nntp Seconds	Threshold: NNTP Seconds	NNTP seconds exceeded historical profile threshold for private side address
NntpConnections	Threshold: NNTP Connections	NNTP connections exceeded historical profile threshold for private side address
RootFailed	Root failed authentication	Failed root login on firewall
SmtpConnections	Threshold: SMTP Connections	SMTP connections exceeded historical profile threshold for private side address
SmtpInBytes	Threshold: SMTP Bytes IN	SMTP Bytes IN exceeded historical profile threshold for private side address
SmtpOutBytes	Threshold: SMTP Bytes OUT	SMTP Bytes OUT exceeded historical profile threshold for private side address
TaggedIpAddr	Traffic To or from a Tagged IP Address	Connection to or from a tagged public side address
TelnetConnections	Threshold: Telnet Connections	Telnet connections exceeded historical profile threshold for private side address
TelnetInBytes	Threshold: Telnet Bytes IN	Telnet Bytes IN exceeded historical profile threshold for private side address
TelnetOutBytes	Threshold: Telnet Bytes OUT	Telnet Bytes OUT exceeded historical profile threshold for private side

		address
TotalConnections	Threshold: Total Connections	Total connections exceeded historical profile threshold for private side address
TotalInBytes	Threshold: Total Bytes IN	Total Bytes IN exceeded historical profile threshold for private side address
TotalOutBytes	Threshold: Total Bytes OUT	Total Bytes OUT exceeded historical profile threshold for private side address
UnauthConnections	Threshold: Unauthorized Connections	Total unauthorized connections exceeded historical profile threshold for private side address

RAPTOR ALERTS AND WARNINGS

CMDS Alerts for Raptor.

ALERT MESSAGE	DESCRIPTION	INTERPRETATION
AccessDenied	Access denied	Authentication failed for user
Error	Gateway hiccup: error	Internal Raptor error
GwShutdown	Shutdown command received, gwcontrol quitting	User has shut down the Raptor Firewall
ProcessKilled	Unauthorized process killed	User has killed a process he was not authorized to kill
UnknownEntity	Unknown entity connected to readeagle	An unknown entity has connected to the Firewall

CMDS Warnings for Raptor.

WARNING MESSAGE	DESCRIPTION	INTERPRETATION
AolConnections	Threshold: AOL Connections	AOL connections exceeded historical profile threshold for private side address
ConfigFile	Config file not from authorized machine	Firewall detected that config file that was read in was NFS mounted
DenyAccess	Denied access to command	The user has been denied access to a command.
FtpConnections	Threshold: FTP Connections	FTP connections exceeded historical profile threshold for private side address
Http Connections	Threshold: HTTP Connections	AOL connections exceeded historical profile threshold for private side address
NntpConnections	Threshold: NNTP Connections	NNTP connections exceeded historical profile threshold for private side address
PasswdChange	Password Changed	User has changed password
RemoteConnect	Unauthorized remote connect attempt from host	User has attempted to connect from a remote host
SmtpConnections	Threshold: SMTP Connections	SMTP connections exceeded historical profile threshold for private side address
TelnetConnections	Threshold: Telnet Connections	Telnet connections exceeded historical profile threshold for private side address
TotalConnections	Threshold: Total Connections	Total connections exceeded historical profile threshold for private side address
UnauthConnections	Threshold: Unauthorized Connections	Total unauthorized connections exceeded historical profile threshold for private side address
VerifyEthernet	Cannot verify ethernet address	The ethernet address to which Raptor is attempting to connect canot verified
VPN	VPN authentication failed	User has entered a VPN site which has failed authentication

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. ERROR MESSAGES. [Ref. 13]

Historical profile error messages

Message	Cause
x Error: User Name, Target, Start and End Date must be specified.	You did not enter any inputs for user name, target machine name, start or end date.
x Error: Date not in CCYYMMDD format.	The start or end date you entered is not in the CCYYMMDD format.
x Error: Date <Date entered> is invalid. Month must be between 1- 12 and Day must be between 1-31.	The start or end date day you entered is less than 1 or greater than 31 or the month you entered is less than 1 or greater than 12.
x Error: Date cannot exceed current date.	The start or end date you entered is greater than today's date.
x Error: End date must be at least one day past the Start Date.	The start date you entered is greater than or equal to the end date.
i No Historical Data was found for <user name> at <target> between <start date> to <end date>.	The historical profile you entered does not exist.
i No Historical Data was found between <date> to <date>.	There is no historical data for the dates you entered.
x Error: Historical Data was found starting at <date data found>.	The start date you entered has no data, so the Historical Profiles function informs you of the date of the first set of data found.

Daily Profile Error Messages.

Message	Cause
x Error: User Name, Target and Date must be specified.	You did not enter any inputs for user name, target machine name, or date.
x Error: Date not in CCYYMMDD format.	The date you entered is not in the CCYYMMDD format.
x Error: Date <date entered> is invalid. Month must be between 1-12 and day must be between 1-31.	The day you entered is less than 1 or greater than 31 or the month you entered is less than 1 or greater than 12.
x Error: Date cannot exceed current date.	The date you entered is later than today's date.
x Error: Target <target entered> does not exist.	The target you entered does not exist.
i Profile for <user name> does not exist on <date entered> (CCYYMMDD).	The profile you entered does not exist.
x Error: Problems opening Profile Data for <user> at <date>(CCYYMMDD).	The profile data file is corrupt or cannot be read.

LISTS OF REFERENCES

1. Russell, D. and Gangemi, G.T., *Computer Security Basics*, O'Reilly & Associates, Inc., 1991.

2. Myers, P.A., *Subversion: The Neglected Aspect of Computer Security*, Master's Thesis, Naval Postgraduate School, Monterey, California, June 1980.

3. White, G.B., Fisch, E.A., and Pooch, U.W., *Computer System and Networks Security*, CRC Press, 1996.

4. Irvine, C.E., Stemp, R., and Warren, D.F., *Teaching Introductory Computer Security at a Department of Defense University*, Naval Postgraduate School, Monterey, California, 1997.

5. INFOSEC Technical Assistance Center (ITAC), "INFOSEC Tip of the Week Number 17 - Analyzing Internal Threats "The Enemy within"," [http://infosec.navy.mil/TEXT/tip17.html], July 1999.

6. National Security Agency, *The Inside Threat to United States Government Information System - Draft Report*, pp. 2-28, Government Printing Office, Washington, D.C., 1998.

7. Purcell, Michael, Austin, Tom, Stokey, Roger, von Alt, Chris, and Prada, Ken, "A Vertical Profiling System for Making Oceanographic Measurements in Coastal Waters," IEEE, 1997.

8. Hong, S.B. and Kim, Kapsu, "Classifying and Retrieving Software Components Based on Profiles", paper presented at the Information, Communications and Signal Processing, ICICS '97 convention in Singapore, 9-12 September 1997.

9. McClure, Carma, "Recent Books and Papers," [http://www.reusability.com/papers.html]. 1998.

10. Coast Audit Trail Reduction Group, "Audit Trail Reduction," [http://www.cs.purdue.edu/coast/projects/audit-trails-reduce.html]. December, 1998.

11. Informer Systems Limited, "Secure-IT 2000 Authentication," [http://www.informer.co.uk.sit2000a.html]. 1997.

12. Jain, Raj, *The Art of Computer Systems Performance Analysis,* John Wiley & Sons, Inc., 1991.

13. ODS Networks, Inc, "Computer Misuse Detection System Users Guide, Version 3.5.1," 1998.

14. Krause, Micki and Tipton, H.F., *Handbook of Information Security Management 1999*, CRC Press, 1999.

15. Garfinkel, Simson and Spafford, Gene, *Practical Unix & Internet Security*, O'Reilly & Associates, Inc., 1996.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center..2
   8725 John J. Kingman Rd., STE 0944
   Ft. Belvoir, Virginia 22060-6218

2. Dudley Knox Library..2
   Naval Postgraduate School
   411 Dyer Rd.
   Monterey, California 93943-5101

3. Superintendent...1
   Attn: RADM Robert C. Chaplin
   Naval Postgraduate School
   Monterey, CA 93943

4. Chairman, Information Warfare Academic Group......................................1
   Naval Postgraduate School
   Root Hall, Room 201D
   Monterey, CA 93943

5. Director, National Security Agency...1
   Attn: Lt Gen Michael V. Hayden, USAF
   9800 Savage Road
   FT. Meade, MD 20755

6. Commander, Naval Security Group Command..1
   Attn: RADM Winsor Whiton
   9800 Savage Road
   FT. Meade, MD 20755

7. Director, National Security Agency...1
   Attn: IOTC/CAPT Ken Verbruge
   9800 Savage Road
   FT. Meade, MD 20755

8. Director, National Security Agency...1
   Attn: C4/Mr. Steve Lafountain
   9800 Savage Road
   FT. Meade, MD 20755

9. Director, National Security Agency...1
   Attn: K51/Mr. Robert Eubank
   9800 Savage Road
   FT. Meade, MD 20755

10. Director, National Security Agency...1
Attn: Z6/Mr. Francis landolf
9800 Savage Road
FT. Meade, MD 20755

11. Director, National Security Agency...1
Attn: Z7/Mr. Lew Shipp
9800 Savage Road
FT. Meade, MD 20755

12. Director, National Security Agency...1
Attn: X6/CAPT Edwin Kanerva
9800 Savage Road
FT. Meade, MD 20755

13. Director, National Security Agency...1
Attn: P4/CAPT Miriam Perlberg
9800 Savage Road
FT. Meade, MD 20755

14 LT Stephen E. Mills..1
1515 Dinwiddie ST
Sterling, VA 20164

15 LT Scott Graham..1
207 Normandy RD
Seaside, CA 93955